



April 4, 2024

RESPONSE TO: CRFP 0947 ERP2400000002  
Technical Proposal

Identity Management Single Sign-On Solution  
West Virginia Purchasing Division

Submitted To: Larry D. McDonnell  
304.558.2063  
Larry.d.mcdonnell@wv.gov

Submitted By: Clango, Inc.  
2107 Wilson Blvd., Suite 250  
Arlington, VA 22201  
703.524.3309 (p)  
[www.clango.com](http://www.clango.com)

Contact Person: Duane Graham, CEO  
dgraham@clango.com

Vendor Signature:

Date: April 4, 2024

**BID RECEIVED LATE**  
BUYER   
WITNESS   
**DISQUALIFIED**



RECEIVED

2024 APR -5 PM 3: 56

WV PURCHASING  
DIVISION

---

## Contents

Transmittal Letter .....	1
1 Executive Summary .....	2
2 Designated Contact .....	4
3 Addendum Acknowledgement .....	5
4 Certification and Signature .....	6
5 CyberArk Identity Solution Capability .....	7
5.1 CyberArk Identity – Core Features .....	8
5.1.1 Single Sign-On (SSO) .....	8
5.1.2 Secure Web Sessions (SWS) .....	9
5.1.3 Workforce Password Management .....	10
5.1.4 Adaptive Multi-Factor Authentication (MFA) .....	11
5.1.5 Identity Users – B2E, B2C, B2B .....	13
5.1.6 Identity Lifecycle Management (LCM) .....	14
5.1.7 Identity Flows .....	15
5.1.8 Identity Compliance .....	15
5.1.9 Directory Services .....	16
5.2 CyberArk Identity – Platform Overview .....	17
5.2.1 Service Architecture .....	17
5.2.2 Directory Service .....	18
5.2.3 Policy Service .....	19
5.2.4 Federation Service .....	19
5.2.5 Workflow Service .....	19
5.2.6 Reporting Service .....	19
5.2.7 Browser Extension and Password Vault Service .....	20
5.2.8 User Behavior Analytics Service .....	20
5.3 User Facing Components .....	21
5.3.1 Identity Mobile App .....	21
5.3.2 Windows and Mac Agents .....	21

5.3.3	Admin Portal .....	21
5.3.4	User Behavior Analytics Portal.....	21
6	Proposed Approach and Methodology.....	22
6.1	Project Management Approach.....	22
6.2	Tailored IAM Implementation Methodology .....	23
6.3	Expected Level of Client Engagement.....	24
6.4	Data Prep and Process Reviews .....	24
6.5	Project Team Structure .....	25
6.6	Proposed Implementation Plan .....	26
6.6.1	Phase 1: Project Kickoff, Discovery & Workshops.....	27
6.6.2	Phase 3: Application Setup & Configuration.....	30
6.6.3	Proposed Project Schedule .....	31
6.7	Managing Implementation Risks .....	32
6.8	Mitigating Common IAM Implementation Risks.....	32
6.9	Quality Control Methods .....	34
6.10	Resolution of Blockers and Implementation Activities.....	35
6.11	Change Management and Communications .....	36
6.12	Training .....	37
6.13	CyberArk OEM Support.....	38
7	Experience and Qualifications .....	38
7.1	Corporate Information Summary .....	38
7.2	Clango Corporate Qualifications .....	39
7.2.1	Relevant Experience – Public Sector.....	39
7.3	Qualifications of Staff.....	41
7.4	Proposed Project Personnel (Resumes).....	42
7.4.1	Thomas Yee (Project Manager).....	42
7.4.2	Dan Ross (Identity Security Architect) .....	44
7.4.3	Son Pham (Senior Identity Security Engineer).....	48
7.5	Clango Services References .....	51
7.5.1	State of Illinois .....	51

---

7.5.2	State of Delaware.....	53
7.5.3	Minnesota State University .....	54
7.6	CyberArk Identity Solution References.....	56

***Request for Confidentiality***

*Clango, Inc. believes the contents of this document are valuable and could damage its business if revealed to its competitors. Accordingly, all pages of this response have been submitted in confidence. The data presented herein contains privileged or confidential information. Such data shall be used only for evaluation purposes. However, if a contract is awarded to Clango as a result of, or in conjunction with the submission of this document, The State of West Virginia shall have the right to use or disclose the data contained herein to the extent provided in the contract.*

*Clango reserves the right to modify this response as it identifies, through discussions and negotiations with The State of West Virginia, any changes in the requirements scope, timing, and associated costs.*

---

## Transmittal Letter

Clango, Inc.  
2107 Wilson Boulevard, Suite 250  
Arlington, VA 22201  
April 4, 2024

Larry D. McDonnell  
The State of West Virginia Department of Administration  
Purchasing Division  
2019 Washington Street East  
Post Office Box 50130  
Charleston, WV 25305-0130

Reference: Response to CRFP-0947-ERP2400000002

Dear Mr. McDonnell:

Clango, Inc. is pleased to present our proposal for the above referenced RFP for The State of West Virginia Department of Administration, Purchasing Division Identity Management Single Sign-On Solution.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Please feel free to contact me directly should you have any questions concerning this response or any relevant aspects of our organization, our vendor partner, or our combined experience.

Very Truly Yours,



Duane Graham, CEO

E-mail: [dgraham@clango.com](mailto:dgraham@clango.com)

Phone: (703) 524-3309

## 1 Executive Summary

Clango, Inc. is a pure-play Identity Security services company. Our unified Identity Security solutions protect identities throughout their lifecycle and across the ecosystem by joining the end-to-end capabilities of Identity and Access Management (IAM), Privileged Access Management (PAM), and Identity Governance and Administration (IGA). Over our 30 years of continuous operations, we have delivered market-leading identity security solutions (IAM/IGA and PAM) and advisory services on more than 1,200 distinct client projects, leveraging our experience and vendor relationships with the

industry-leading identity security software products. Our long history of success providing IAM and PAM implementation and advisory services to our clients demonstrates our proven, repeatable approach and customer-first commitment to helping our clients achieve and realize lasting value from their identity security initiatives. In the previous two years (2021-2022), Clango completed more than 400 projects across the privileged access and identity management landscape, crossing a corporate milestone of **successfully delivering more than 1,200 total identity security client projects since 2015**.

Recognized by Gartner for IAM professional services and backed by more than 16 of our overall 30 years of corporate experience successfully delivering IAM professional services, we are confident in our ability to provide the State with the specialized skills, capabilities, and experience outlined in the RFP. Our services, capabilities, and areas of specialization within IAM are listed below:

### Why Clango?

- **Successful completion of more than 225 identity security engagements in the past year** (Identity and Access Management, Identity Governance and Administration, Privileged Access Management, and Identity Advisory).
- A **team of highly trained and experienced cybersecurity engineers, architects, advisors, and developers** who have delivered solutions and services over Clango's 30-year history.
- An Identity Security practice that is **recognized as a top Identity and Access Management (IAM) professional services consulting firm** by leading analysts.
- **Considerable customer experience**, proudly serving the IAM and PAM needs of more than 550 distinct clients since 2015, including some of the most complex implementations and integrations within the markets we serve.

IAM Rationalization	Access Governance
Strategy, Planning, & Roadmap Development	Role Based Access Control Design & Engineering
Technology Solution Evaluation	Certifications
Architecture & Implementation	Identity Lifecycle Management
SWOT Assessment	User & Account Provisioning
User Community Definition	Authentication Services
Identity Assurance	Federation/SSO/TFA
RFO Development Assistance	Privileged Access Administration

---

Our team recognizes that determining the optimal IAM / SSO solution and executing effective transformation demands significant expertise and experience. Identity Security, and specifically Identity Security Solutions (IAM/IGA/PAM), have been Clango's focus for the past 16+ years and are the sole focus of our partner CyberArk. This combined experience and expertise has given us a unique perspective in architecting solutions, developing approaches to IAM objectives for customers, and performing enterprise implementations in complex multi-vendor environments. In partnering with The State of West Virginia, we can draw from a set of proven strategies and strengths that are a result of our direct, hands-on experiences working with similar customers. We bring the following guiding principles to each engagement:

- **Looking at IAM as an enabler for cybersecurity and business operations to ensure value and visibility to stakeholders.**
- **Not assuming a technology platform can fulfill all the IAM requirements to lead to maturity.** Clango's years of experience highlight the importance of measuring and displaying progress continuously so value realization to the customer is not static.
- **Relying on a solution-centric approach where best of breed products may need to be integrated for their best features** rather than excessive customization that will make the overall environment unstable.
- **Recognizing that an IAM roadmap must change dynamically to accommodate various drivers that are important to respective influencing parties.** Often, a strategic roadmap is perceived to be a static document. This can lead to inflexibility and failure.
- **Experience and exposure to many relevant use cases and best practices** that organizations pursue for an effective IAM program.
- **Leveraging industry-leading IAM Advisory Consulting + highly experienced and credentialed Professional Services** to provide our customers with a partnership approach to all our engagements, integrating best-practice IAM/IGA advisory services with expert technical implementation capabilities – *uniquely positioning Clango to bring value across the entire organization.*

To satisfy the RFP requirements and deliver a best-value solution, we are proposing **CyberArk's** industry-leading **Access Management** and **Identity** SaaS solution. This CyberArk product will provide the State with a market-leading, modern identity management solution that streamlines operations and gives workers simple and secure access to all their enterprise resources – on-premises, cloud, hybrid – from any location, using any device. The solution will enable users to effectively – *and efficiently* – participate in a wide variety of Identity and Access Management (IAM) processes, including automated access certifications, policy management, access request and provisioning, password management, and identity intelligence. With resource connectors included as part of the base platform, the product delivers out-of-the-box integration to a wide variety of applications running in the datacenter or the cloud.

## 2 Designated Contact

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administration and the initial point of contact for matters relating to this Contract.

<b>Name and Title</b>	Patrick McGeehan, VP of Service Delivery
<b>Address</b>	2107 Wilson Blvd. Suite 250 Arlington VA 22201
<b>Phone Number</b>	571-483-2727
<b>Email Address</b>	pmcgeehan@clango.com



### 3 Addendum Acknowledgement

**ADDENDUM ACKNOWLEDGEMENT FORM**  
**SOLICITATION NO.: CRFP ERP24\*02**

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**

(Check the box next to each addendum received)

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6  |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7  |
| <input type="checkbox"/> Addendum No. 3            | <input type="checkbox"/> Addendum No. 8  |
| <input type="checkbox"/> Addendum No. 4            | <input type="checkbox"/> Addendum No. 9  |
| <input type="checkbox"/> Addendum No. 5            | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Clango, Inc

\_\_\_\_\_  
Company



\_\_\_\_\_  
Authorized Signature

April 4, 2024

\_\_\_\_\_  
Date

**NOTE:** This addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 6/8/2012

## 4 Certification and Signature

**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Clango, Inc

(Company)



(Signature of Authorized Representative)

Duane Graham, CEO April 4, 2024

(Printed Name and Title of Authorized Representative) (Date)

703-524-3309

(Phone Number) (Fax Number)

dgraham@clango.com

(Email Address)

## 5 CyberArk Identity Solution Capability

CyberArk Software was founded in 1999 with the vision of protecting high-value business data and pioneering Digital Vault technology. CyberArk acquired Idaptive software in 2020 - a market leader in Identity as-a-Service offerings. Together, CyberArk and Idaptive, now named as **CyberArk Identity**, provide a comprehensive Artificial Intelligence (AI) based, security-first approach to managing Identities that is adaptive and context-aware, and architected on the principles of Zero Trust and Least-Privilege access.

**CyberArk Identity** is a dedicated Access Management and Identity Management solution. With CyberArk Identity, organizations can enhance security and improve end-user productivity by reducing the number of credentials a user needs to remember and tying all application accounts to a single identity. Organizations can then leverage the solution's Adaptive Multi-Factor Authentication capabilities to secure all user identities and leverage risk-based, contextual access controls to ensure all users are who they say they are, without overburdening them with unnecessary authentication steps.

We believe the features and capabilities of **CyberArk Identity** described below deliver the foundational components of a successful Identity program. As each member of the State's team reviews the information, our request is that you remember that all the features and capabilities that are delivered in the CyberArk Identity solution are built with a security-first perspective. In some markets, there is a preference for convenience over security, yet we believe the user experience should not be too cumbersome - otherwise, users will be slow to adopt identity-management controls or attempt to circumvent policies. With the CyberArk solution, the State will reap the benefits of both security and convenience.

### CyberArk Identity Certifications & Compliance



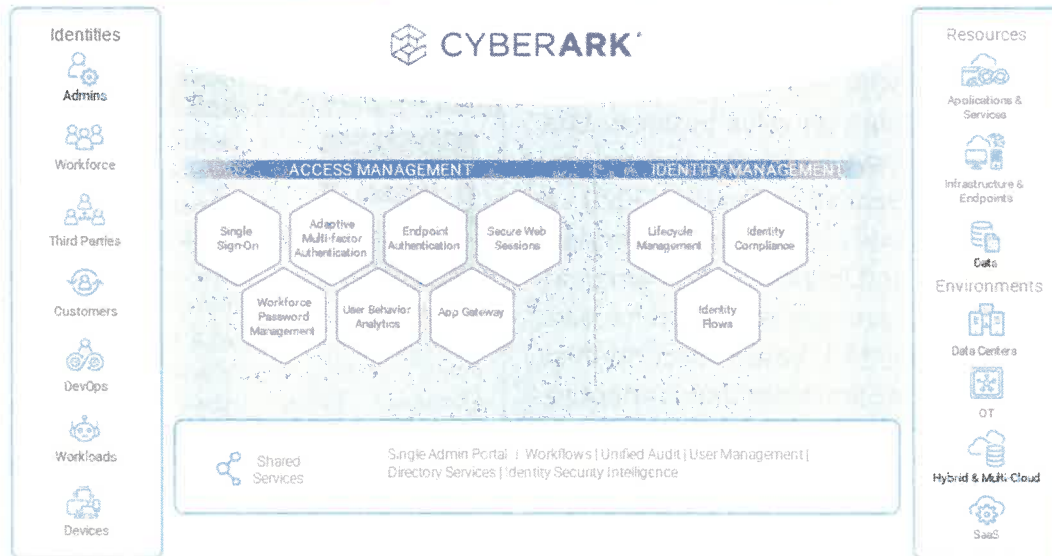
FedRAMP

CyberArk Identity has achieved Federal Risk and Authorization Management Program (FedRAMP) High authorization to operate (ATO) status. This authorization reinforces CyberArk's ability to help public sector organizations efficiently and effectively secure access to all corporate applications, protect distributed workforces and accelerate cloud innovation in alignment with Zero Trust principles.

FedRAMP authorized solutions ensure that the product meets stringent security and compliance standards set by the U.S. federal government, significantly reducing the risk of security breaches and data compromises. It also streamlines the approval process for government and public sector agencies to adopt cloud services, saving time and resources while ensuring that sensitive information is protected according to federally mandated guidelines.

#### Additional Certifications and Compliance:

- GDPR
- ISO 27001 :2013
- ISO 9001:2015
- **SOC 2 Type II**
- CSA STAR Level 1



The solution also enables IT organizations to manage user on-boarding/off-boarding workflows and automatically provide role-based access to business-critical applications. This ensures that all users have the correct access to applications necessary to do their job on day one and conversely that users who have left the organization no longer have access to sensitive data. The breadth of the solution, represented in the graphic above, will allow the State’s IAM program to mature using a single-vendor platform.

## 5.1 CyberArk Identity – Core Features

### 5.1.1 Single Sign-On (SSO)

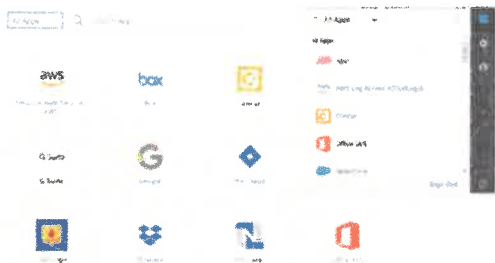
The Single Sign-On offering is an easy-to-manage solution for one-click access to your cloud, mobile, and legacy apps. CyberArk SSO enables a secure and frictionless sign-in experience for both internal and external users that adjusts based on risk. Users simply sign into a web portal using their existing credentials to access all their assigned applications from one place. CyberArk Adaptive SSO uses machine learning to build a baseline profile for each user, leveraging location, device, network, time-based, and user-specific contextual attributes. This enables organizations to analyze user activity against historical patterns, assign risk to each access request, and create policies and actions that are triggered when anomalous behavior is detected.

# Single Sign-On

Drive employee productivity, reduce help desk calls, and demonstrate compliance

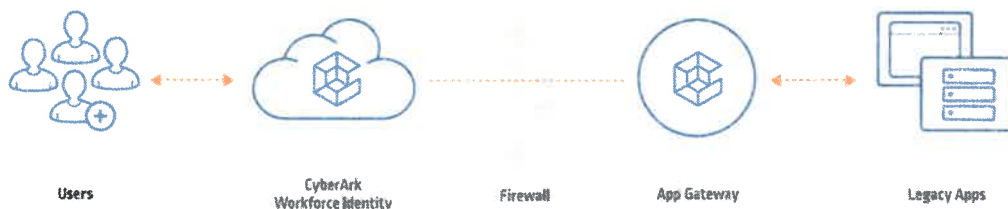
## Enable One-click Access

to your cloud, mobile, and legacy apps



 <p><b>SINGLE SIGN-ON</b>        A single identity to login to all cloud and on-prem apps. Averaging SSO standards.</p>	 <p><b>APP CATALOG</b>        Easy deployment of single sign-on to thousands of pre-integrated web and mobile apps.</p>
 <p><b>SELF-SERVICE PASSWORD RESET</b>        Enable end-users to reset their own passwords and unlock account.</p>	 <p><b>VPN-LESS APP ACCESS</b>        SSO into on-prem apps and enforce access policies without a VPN (App Gateway Service).</p>

App Gateway is an add-on to the Single Sign-On service that enables VPN-less access to legacy on-prem applications. It allows companies to set up per-application, per-user access to individual legacy applications. The access is based on application URLs, users, groups, and network information and allows direct access to applications without exposing the rest of the internal network, installing hardware, or changing firewall rules.



### 5.1.2 Secure Web Sessions (SWS)

Secure Web Sessions enables continuous authentication to ensure that the person who initiated the web session is the one using the application. With SWS, you can monitor, record, audit, and protect end-user activity within designated web applications. The solution uses a browser extension on an end-user’s endpoint to monitor and segregate web apps that are deemed sensitive by enterprise IT, security administrators, and business application owners. Security and compliance professionals can use Secure Web Sessions to efficiently identify anomalous activity, investigate issues, and support audits. In addition, Secure Web Sessions allows you to define

notification and enforcement rules for specific text and number fields within web applications. For example, you can create rules to alert you when users attempt to transfer funds that exceed a pre-set threshold within your banking app or ensure that only users with your company's email domain can be added to your cloud management console.

## Secure Web Sessions

Record, audit and protect end-user activity within web applications secured by CyberArk Identity



**Context-aware session recording and auditing** without impacting end-user experience.

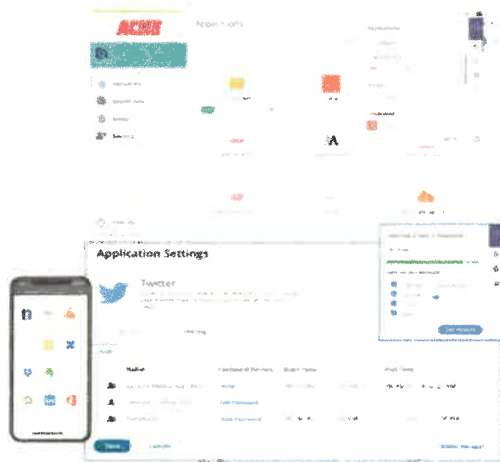
- 
**SESSION RECORDING**  
 Seamlessly record screenshots of all actions taken by specific end-users within protected applications
- 
**AUDIT TRAILS**  
 Easily search recorded sessions using free-text input and quickly filter events by dates and actions
- 
**CONTINUOUS AUTHENTICATION**  
 Automatically determine when end-users walk away, leaving a session open and force them to re-authenticate
- 
**SESSION PROTECTION**  
 Isolate web sessions at the endpoint and prevent end-users from copying data or downloading files

Secure Web Sessions provides visual, in-depth insights, recording end-user actions down to the keystroke without impairing the end-user experience. The solution protects applications against unauthorized access by intelligently detecting open sessions and forcibly re-authenticating users. And it protects web sessions against data exfiltration by restricting downloads and copying of data. In addition, the optional integration with CyberArk Endpoint Privilege Manager defends against malware and other endpoint-originated threats by protecting web sessions and blocking untrusted scripts.





### 5.1.3 Workforce Password Management

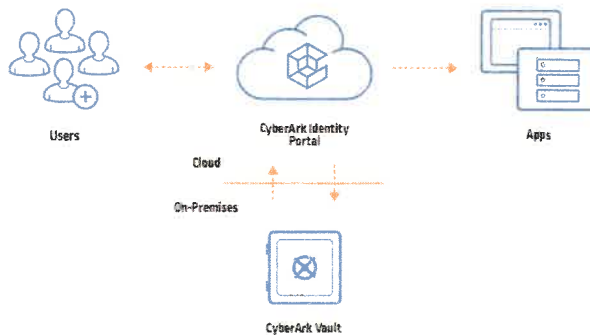
Workforce Password Management capability helps companies overcome the unique user authentication and auditing challenges presented by business applications requiring an individual username and password credentials. With Workforce Password Management, users can quickly add passwords for their business applications to a centralized User Portal, securely access apps with a click of a button, and share access to these apps with other users. Behind the scenes, the passwords are securely stored in the CyberArk Identity Cloud or self-hosted CyberArk Vault.

## Workforce Password Management



Secure and collaborate enterprise and personal application credentials with enhanced end-user access experience.

 <p><b>CENTRALIZED PASSWORD MANAGEMENT</b></p> <p>Single console to federate with IDPs, define security policies and generate security and compliance reports</p>	 <p><b>SECURED ACCESS</b></p> <p>Seamless, zero-knowledge storage and access to business passwords in the self-hosted vault or in the cloud</p>
 <p><b>PASSWORD COLLABORATION</b></p> <p>Secure passwords to collaborate with other users in the organization and governance</p>	 <p><b>REPORTING AND VISIBILITY</b></p> <p>Track access activity, control password complexity, and revoke access to applications when no longer needed</p>



The included CyberArk Identity Browser Extension automatically recognizes when new passwords are entered, helps generate complex passwords, saves them in the cloud or self-hosted vault, and adds application shortcuts to users' individual User Portals. End-users simply click on app shortcuts to launch applications, and Browser Extension opens login pages and fills out stored credentials.

### 5.1.4 Adaptive Multi-Factor Authentication (MFA)

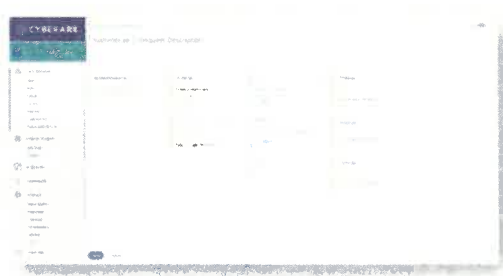
Adaptive MFA enables enterprises to enforce risk-aware, strong identity assurance controls within the organization to validate users. CyberArk Adaptive MFA supports the broadest range of authentication factors, including passwords, One-Time Passwords (OTP) push notifications, and hardware cryptographic devices, such as YubiKeys. Our adaptive MFA solution also supports passwordless authentication factors, such as QR codes and on-device biometric factors (Windows Hello, TouchID). In addition, all MFA profiles display the minimum and maximum AAL

(Authenticator Assurance Level) to make it easier for organizations to adopt stronger and more secure authentication processes based on National Institute of Technology (NIST) standards.

CyberArk Adaptive Multi-factor Authentication solution supports the widest range of use cases, including cloud and on-premises applications, laptops and desktops, VPNs, 3rd party proxies, and even other Identity Providers (IDPs). One of the big differentiators for MFA capability is the seamless integration with our CyberArk User Behavior Analytics (UBA) service to provide risk-based authentication. CyberArk UBA uses artificial intelligence and machine learning to develop profiles for each of the users and can spot behavior that does not match historical activities. This means that depending on the specific contextual information available about the user, device, and access request you can dynamically enforce stronger secondary authentication requirements or, conversely, relax your controls for low-risk access attempts.

## Adaptive Multi-Factor Authentication

Strengthen security through high authentication assurance and drive superior user experience



Provide Identity Assurance  
before granting access to corporate applications



As mentioned earlier, User Behavior Analytics enables you to determine the risk of every user and access request by collecting and analyzing a rich set of contextual information. The UBA engine builds user profiles that model standard behavior and automatically flags anomalous activity. With UBA, you can generate identity intelligence insights, investigate security incidents, and define remediation actions when potential breach attempts are detected.

The User Behavior Analytics engine powers our SSO and MFA solutions and helps customers to improve user experience without compromising security. For example, with UBA, you can present users with the level of authentication friction that is commensurate with the amount of risk posed by the user. Meaning low-risk access attempts can require a simple username and password combination, while high-risk access requests to sensitive resources would require step-up authentication with a physical token.



### **5.1.5 Identity Users – B2E, B2C, B2B**

User types are essential for understanding the different interactions a business has and the various cybersecurity and identity management solutions that may be needed to support these interactions securely.

B2E (Business-to-Employee) refers to the internal operations and transactions within a business that are directed towards the employees. B2E user types are authorized users that are employees of a customer or its affiliates. They may require access to internal systems, applications for productivity, communication, HR services, and more.

B2C (Business-to-Consumer) involves transactions or interactions between a business and individual consumer. B2C user types are the customers or consumers who utilize a service offered by a business or its affiliates. This can include online shopping, service subscriptions, or any direct sales from business to the end consumer.

B2B (Business-to-Business) refers to transactions or interactions between two businesses, such as between a manufacturer and a wholesaler, or a wholesaler and a retailer. B2B user types typically include authorized users that are third-party consultants, contractors, or vendors of a customer or its affiliates. They may require secure access to certain applications or systems relevant to their business dealings.

Now more than ever, an organization's success is increasingly dependent on collaborating with other businesses. For example, you may need to work with business partners, communicate with 3rd party vendors, place orders with suppliers, or oversee supply chain operations with distributors. This means you must be prepared to securely share access to your company applications and services while maintaining control over your corporate data or face the risk of security breaches.





CyberArk B2B Identity allows you to extend secure and seamless access to your SaaS applications for your business partners, vendors, and clients. With B2B Identity, you can authenticate, authorize, and manage your B2B identities to govern and secure external access, mitigate business risk, reduce admin and developer costs, and build scalable applications and portals.

## B2B Identity

Authenticate, authorize, and manage your B2B identities and access to SaaS applications to provide a secure and seamless experience



### Fast and frictionless access to your SaaS applications for your business partners, vendors, and clients

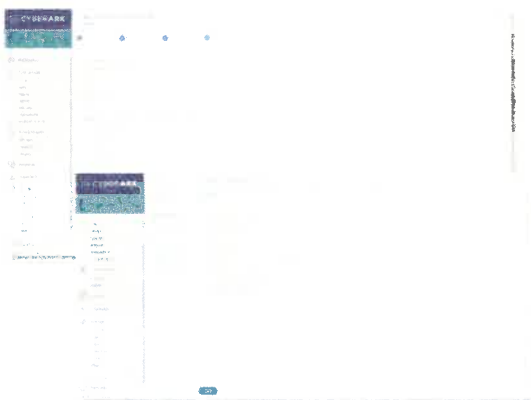
 <p><b>SIGN-UP &amp; AUTHENTICATION</b> Add onboarding and strong authentication to your web &amp; mobile apps within minutes</p>	 <p><b>APPLICATION ACCESS SECURITY</b> Secure access to applications or sensitive step-up workflows using standards such as OAuth, OIDC, and SAML</p>
 <p><b>DELEGATED ADMINISTRATION &amp; FEDERATION</b> Easily and securely scale B2B identity administration to partner admins</p>	 <p><b>LOW CODE WIDGETS &amp; DEVELOPER TOOLKITS</b> Build personalized authentication and user portals using web &amp; mobile SDKs</p>

### 5.1.6 Identity Lifecycle Management (LCM)

CyberArk Identity Lifecycle Management solution provides an easy way to route application access requests, create application accounts, manage entitlements for those accounts, and revoke access when necessary. With Lifecycle Management, you can enable users to request access to applications from the CyberArk Identity App Catalog, provide specific users the ability to approve or reject these access requests, and automatically create, update, and deactivate accounts based on user roles.

## Identity Lifecycle Management

Automate access for joiner, mover, leaver use cases



### Provision Access to Cloud, Mobile and On-Prem Apps from a central administration point

 <p><b>AUTOMATE ACCESS PROVISIONING</b> Provision users &amp; apps with the right access based on roles and groups</p>	 <p><b>DYNAMIC POLICY-BASED ACCESS CONTROLS</b> Automate licensing and entitlement and manage device authorization</p>
 <p><b>HR-DRIVEN IDENTITY</b> Leverage HR systems as the single source of truth</p>	 <p><b>CUSTOM APP INTEGRATIONS</b> Automatically create accounts and integrate custom apps</p>

CyberArk Identity LCM also provides the ability to seamlessly import identities from your preferred HR system or application, such as Workday, UltiPro, BambooHR, or SuccessFactors, and

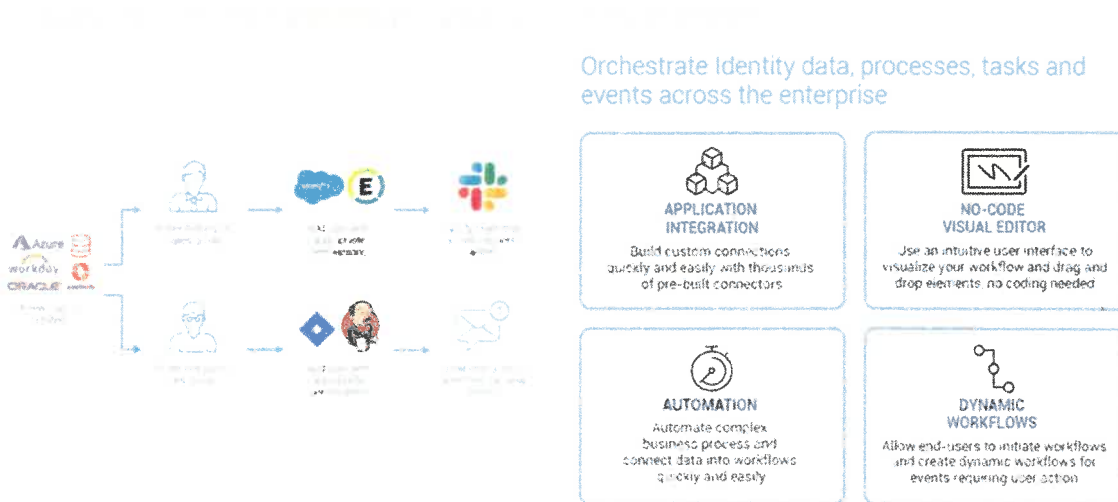
provision them to your Active Directory or CyberArk Identity Cloud Directory. This enables you to unify your provisioning and HR workflows and have an HR-driven primary system of record for user data across all enterprise applications.

### 5.1.7 Identity Flows

CyberArk Identity Flows allows organizations to eliminate manual tasks and processes by automating complex identity management workflows. It's quick, easy and cost-effective. A no-code visual editor and thousands of prebuilt connectors make it possible to rapidly orchestrate identity events, build workflows, and synchronize identity data across diverse applications, directory stores, and repositories.

With Identity Flows, you can automate routine IT and security operations, increase visibility and control, improve efficiency, and reduce risk. The solution is ideal for creating workflows for various use cases, including identity lifecycle management automation, responding to risk with adaptive access control, and streamlining complex business processes.

## Identity Flows



### 5.1.8 Identity Compliance

CyberArk Identity Compliance provides a single view of who has access to what — and makes it easier for organizations to enforce and demonstrate compliance by continuously discovering access, streamlining access certifications and providing comprehensive identity analytics.

Identity Compliance automates manually intensive, error-prone administrative processes, ensuring that all access rights are properly assigned and continually certified across the extended

enterprise. The solution helps contain identity sprawl and apply the principles of least privilege across today’s highly distributed, hybrid IT environments. Identity Compliance is delivered as a cloud-based service for rapid deployment, easy operation and fast time-to-value.

## Identity Compliance



Identity Compliance also enables the certification of access. For example, the organization can require managers to review and certify user access to a specific set of applications — or for certain roles or user groups on a monthly or quarterly basis, as required by various regulatory bodies. Administrators can also apply controls such as risk-based reviews or can require multi-factor authentication (MFA) for the certifier. Identity Compliance keeps auditors happy by providing an easy-to-use and customizable dashboard with analytics.

### 5.1.9 Directory Services

CyberArk Directory Services enable you to consolidate all identity siloes within the enterprise without requiring you to duplicate identities in the cloud. You can easily create, import, or federate identities from any number of sources without replicating user data.

Our cloud architecture can work seamlessly with any existing directory, enterprise or social or a federated directory or you can leverage our own highly scalable and flexible cloud directory.

## Directory Services

Consolidate identities without relinquishing control



### Integrate With On-prem or Cloud Directories to store identity data



#### IDENTITY WHERE YOU CONTROL IT

Create or import identities from any number of sources without replicating user data in the cloud



#### INFINITE SCALABILITY

Dynamically scale up or the number of users for all use cases: workforce, partners and consumers



#### CLOUD/ON-PREM DIRECTORY SUPPORT

Integrate with 3-party directory services including AD, Azure AD, and Google Directory



#### EXTENSIBLE DIRECTORY SCHEMA

Leverage the directory for users, computers, endpoints, mobile and server objects with custom schemas

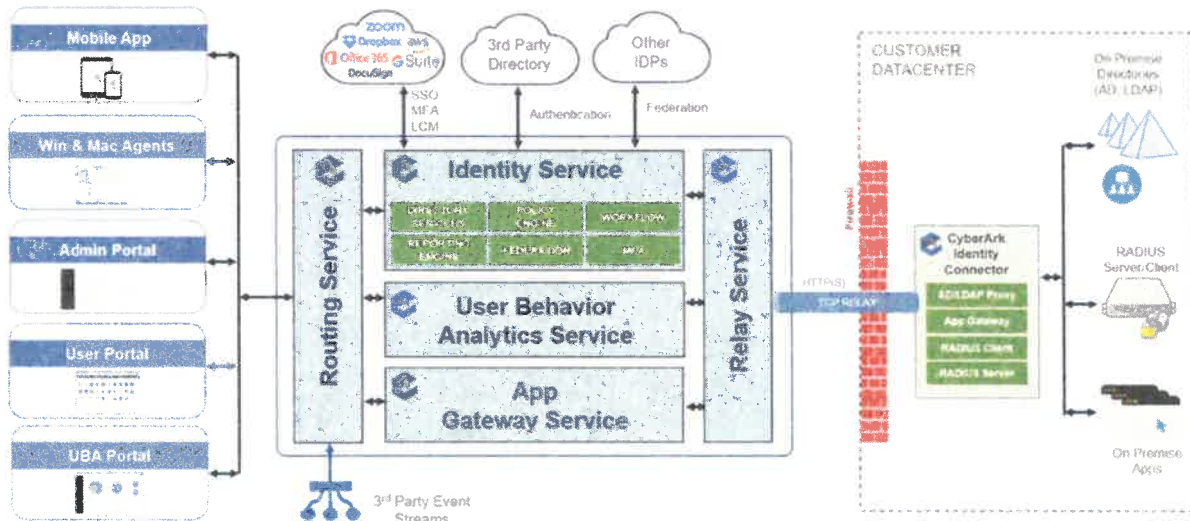
## 5.2 CyberArk Identity – Platform Overview

### 5.2.1 Service Architecture

This section details the CyberArk Identity cloud architecture. CyberArk Identity acts as a client to a customer's internal Active Directory or LDAP system and uses strong encryption to ensure user data remains secure. With CyberArk Identity, Active Directory and LDAP data remains protected within the customer's environment without requiring replication to the cloud. CyberArk simply accesses Active Directory or LDAP data in place and, while some minimal amount may be cached for performance reasons and faster access, it is meticulously protected. Notably, credentials are never cached for security reasons.

In addition, no user data is cached or stored on users' mobile devices or within any browser. CyberArk Identity customer data is always encrypted with AES 256-bit encryption (in transit and at rest), while cloud hosted data is encrypted with HTTPS mutual authentication.

Each customer data is encrypted with the customer's unique encryption access key. The customer's encryption keys are encrypted with a Pod Master Key and stored in the Pod configuration database, away from the customer's tenant database. Only the CyberArk Identity Operations Team has access to the maintenance tools which can only be used to access customer data where required to provide service for our customers under strictly controlled and audited conditions that are certified under SOC2.



### 5.2.2 Directory Service

A unique capability of CyberArk Identity is the ability to choose where to store the directory — either on-premises (within corporate control), in the cloud, or a combination of both. CyberArk Identity integrates the CyberArk Identity Cloud Directory with Active Directory or LDAP without breaching the corporate firewall or adding devices in the DMZ. Unlike other solutions, CyberArk does not add the security risk of duplicating Active Directory or LDAP records into the cloud, and thus maintains an organization’s identity inside its on-premises directory service (Active Directory or LDAP). The CyberArk Identity’s live connection to Active Directory or LDAP, with automatic load balancing and failover, ensures that Active Directory and LDAP data is highly available and kept safe and in corporate control.

The CyberArk Identity Directory Service can optionally store external users’ identities in the cloud if customers do not have Active Directory or LDAP or want to extend applications to external users (such as customers, contractors, or partners) who are not located on-premises.

In addition, the CyberArk Identity Directory Service uniquely unifies cloud app and mobile management into an enterprise cloud service. CyberArk leverages identity to secure and manage users’ access to applications from any device, regardless of location.

By leveraging a single identity across cloud, mobile and onsite apps, users get a single username and password across all the apps they access for work and IT can enforce consistent access policies based on user identity.

---

### **5.2.3 Policy Service**

The CyberArk Identity Policy Service is a cloud service to enroll devices and can leverage the Connector service for a live connection to Active Directory to extend the power, familiarity and flexibility of Active Directory group policy or the Policy Engine can optionally be run entirely from the cloud without the requirement for, or dependence on Active Directory. The Policy Engine also allows the rich expression of authentication policies such as multi-factor authentication and per-app access control. The policy service stores all the policy information in a database, but also caches the data in a highly scalable and fast Redis cache. The cache allows the policy decision engine within the service to do fast lookups of policies, compute the decision associated with the policy and respond to the client or enforcement point.

### **5.2.4 Federation Service**

CyberArk Identity Federation Service enables both in-bound federation as well as outbound federation. In-bound federation enables end users who are managed and whose identities are stored in third party identity providers to gain access to applications that may be managed by CyberArk. Similarly, outbound federation enables end users who are managed by the CyberArk Identity to gain secure access and single sign-on to third party service providers. CyberArk Identity supports a variety of standards and protocols for federation such as SAML 2.0, WS-Federation, OAuth2, OpenID Connect and WS-Trust.

### **5.2.5 Workflow Service**

CyberArk Identity provides flexible workflow service that powers many features within the Identity Lifecycle Management solution such as application access request workflows, endpoint enrolment workflows and more. The service enables multi-level approvals, auditing, and reporting, is also integrated with the CyberArk Identity mobile app, and supports time-bound approvals.

### **5.2.6 Reporting Service**

CyberArk Identity Reporting service is exposed via the Admin Portal with a browser-based interface for reporting that offers both pre-canned and ad-hoc reporting capabilities. The reports provide real-time views of user activity, administrative activity, application access, mobile devices, and system event information. More than 70 pre-configured reports are available for answering common questions and administrators can customize or create ad hoc report queries based on industry standard SQL from within the reporting interface.

Unique to CyberArk Identity reporting is that known table types are actionable and drillable (Devices, Users, Apps, Roles). So, if a report result contains a column of information from one of these object types, actions can be taken on those objects right in the report or can be cross-linked into the specific administrative views for that object.

Custom reports can be kept private to each individual user or can be leveraged by others through role-based report sharing. Report permissions include read only, read/write and ownership by

---

---

role. Report results will obey all other data access permissions to prevent reporting from circumventing delegated administrative controls. Reports can be organized by folders with role-based access control and are exportable to CSV/Excel or via email.

### **5.2.7 Browser Extension and Password Vault Service**

CyberArk Identity includes a password vault and a browser extension that leverages the password vault for authentication to single sign-on enabled applications (e.g., ones using SAML or Kerberos) as well as other web-based applications that only support a username and password authentication. These web site specific credentials are only decrypted within the service and inserted into the browser for login to the appropriate site over an HTTPS connection. This special field encryption model ensures that access to the information can only be used for the intended purpose defined within the service and that data is protected for misuse or accidental exposure.

### **5.2.8 User Behavior Analytics Service**

CyberArk Identity User Behavior Analytics (UBA) is a cloud service that enables IT Administrators and Security Operations Analysts to continuously visualize and analyze user activity in their organizations, gain instant visibility and insights into anomalous and risky user behavior, and protect sensitive data, applications, and infrastructure from unauthorized access and breaches.

CyberArk Identity UBA provides a variety of built-in reports and dashboards built on a flexible and customizable widget framework. The widget framework enables IT Administrators and Security Operations Analysts to create their own widgets leveraging the visualizations and charts available within the service and compile these widgets into custom reports and dashboards. The service also provides for intuitive data exploration by allowing users to build custom queries on the service's data model, drill down on or rolling up user activity information. These capabilities together enable IT Administrators and Security Operations Analysts to continuously visualize and analyze user activity.

The service leverages unsupervised machine learning and artificial intelligence to autonomously analyze each user's activity to determine typical behavior for that user and then continuously compute risk-scores that signal the extent of anomalous behavior displayed by that user. The service provides complete "explain ability" of the risk-score by providing insights into what factors (time, location, device, network, etc.) contributed to the user's risk score. In addition, IT Administrators and Security Operations Analysts can use CyberArk Identity UBA to trace the timeline of the user's behavior leading up to an event with a high-risk score. The service can also leverage feeds from third party threat intelligence vendors in the computation of this risk score. This enables an organization to gain instant visibility into who are their risky users and gather insights into why their behavior is deemed risky.

To respond to high-risk events and anomalous user behavior, CyberArk Identity User Behavior Analytics provides a flexible framework to enable security orchestration and automated responses. This capability can help stop, in real time, unauthorized access to sensitive data, and prevent breaches that can happen because of compromised identities.



## **5.3 User Facing Components**

### **5.3.1 Identity Mobile App**

The CyberArk Identity Mobile App, available for iOS on the Apple App Store, and Android on the Google Play store, provides these primary capabilities:

- Provides a mobile interface for the CyberArk Identity User Portal list of apps for one-click access to web apps.
- Facilitates SSO and certificate-based authentication for rich mobile applications.
- Provides CyberArk Identity Mobile Authenticator push and soft token factor: CyberArk Identity Mobile Authenticator provides an easy-to-use and secure method for one-click authentication for an enrolled mobile device that is on a cellular or data network or a cryptographically secure one-time passcode that can be used even if the device is offline.

### **5.3.2 Windows and Mac Agents**

The CyberArk Identity Windows and Mac cloud agents, available for download from the CyberArk Identity Admin portal, are responsible for capabilities like Passwordless and Multi-factor Authentication to endpoints, Zero Sign-On (X.509 certificate-based authentication) as well as device compliance management.

### **5.3.3 Admin Portal**

The CyberArk Identity Admin Portal unifies admin interfaces for SaaS and mobile app management, application account provisioning/deprovisioning, user identity management, role management, policy management, monitoring/dashboarding/reporting on all user and admin activity and administrative settings.

### **5.3.4 User Behavior Analytics Portal**

CyberArk Identity User Behavior Analytics uses machine learning to assess risk based on constantly-evolving user behavior patterns, then assigns a risk score, and enforces an appropriate decision real-time — determining whether the user's access is granted, requires step-up authentication, or is blocked entirely. Potentially compromised accounts are flagged and elevated to IT's attention in a rich dashboard with drilldown capabilities.

CyberArk Identity includes multiple out-of-the-box dashboards comprised of dozens of pre-canned widgets that measure activity, risk, and more. Dashboards are interactive, filterable, printable, exportable, and customizable using easy and no-code drag and drop. Dashboard data can be exported. Adaptive analytics supports webhooks to easily integrate with third-party systems based on real-time triggers from incoming events.

---

CyberArk Identity also supports integrations with common SIEM vendors like IBM QRadar, Splunk and ArcSight, and has a built-in syslog writer that can connect to other analytics systems with a Syslog server interface.

## 6 Proposed Approach and Methodology

Clango strongly believe that a holistic, collaborative advisory method is the foundation for being able to deliver successful and lasting outcomes for our customers. When considering the criteria for success, our approach is driven by a focus on short-, mid-, and long-term strategic program goals, all in service to operationalize and embed the concepts of Least Privilege, Zero Exception, and Zero Trust within each of our customer’s organizations.

Adoption is the overarching criteria for success for any Identity Management project. For every project, we strive the achieve the following outcomes:

- Integrate Identity Management principles into the overall security governance for the organization, ensuring there is a shared understanding of ongoing values, requirements, policies, controls, and metrics to foster continuous improvement and sustainment of the Identity Management program.
- Ensure there is an effective communication and change management process specific to Identity Management for the purpose of supporting continued adoption beyond the initial “quick wins.” This guarantees that key stakeholders and application owners are aware of changes as the program continues to roll out across the organization, and as additional accounts and applications are onboarded with improved access controls.
- Operationalize a sustainable strategy for the discovery, onboarding, and management of the organization’s accounts, embracing an automated “factory” approach. This strategy will clearly define the attributes and parameters regarding the handling of each account, how the accounts are categorized, to whom they belong, and the set of default controls and policies that are assigned. This will increase the security of the business’ critical assets while reducing the amount of time and expense that is required to onboard new accounts and applications.
- Establish a framework for continuous monitoring to review accounts, roles, responsibilities, and entitlements to ensure that accounts are compliant with established policies and controls.
- Define Key Performance Metrics to measure the effectiveness of the organization’s ongoing IAM and IGA strategy and framework.

### 6.1 Project Management Approach

Clango utilizes management processes based on the guiding principles of the Project Management Institute’s Project Management Body of Knowledge (PMBOK®) as the foundation of all our project management activities. Our integrated project management approach drives task definition, planning, initiation, staffing, execution, performance, control, monitoring, and

reporting for each initiative, ensuring effective on-time and on-budget deliverables. This approach is flexible and allows us to effectively coordinate, maintain, and control multiple project activities at single or multiple locations. We use a formal PMBOK® process to track and control project activities and measure performance across all task assignments. This uniform process is designed explicitly for the identification of activity dependencies and interdependencies across assignments and for the integration of these activities into an overall performance process, ensuring adherence to schedule, cost, and quality metrics.

Our PMBOK® process supports a framework and tailored implementation methodology that has developed over the course of multiple customer Identity Management solution implementations.

Our framework is designed to build efficiency and consistency on achieving project goals and effective delivery of requirements. Our process, approach, and methods ensure we are as effective as possible for every engagement and solution delivery. Our approach provides flexibility and adaptability to different environments within different organizations.

## 6.2 Tailored IAM Implementation Methodology

At Clango we employ a tailored, hybrid approach to IAM implementations, merging the structured phases of the waterfall method with the iterative flexibility of agile. This methodology is especially suited to the complexities faced by large-scale enterprise customers and is what we recommend for this implementation project.

Framework	Principles Employed	Benefits
Waterfall	<ul style="list-style-type: none"> <li>Distinct, milestone-based planning phases</li> </ul>	<ul style="list-style-type: none"> <li>Clear definition of project stages including initiation, requirement and analysis, solution design, system build, testing and training, and go-live.</li> <li>Defined signoff and gate reviews.</li> <li>Rigorous documentation</li> <li>Adherence and alignment with regulatory standards where required.</li> </ul>
Agile	<ul style="list-style-type: none"> <li>Adaptability and continuous stakeholder engagement.</li> </ul>	<ul style="list-style-type: none"> <li>Flexibility to adjust project scope and requirements.</li> <li>Ensures alignment with evolving requirements and stakeholder expectations</li> </ul>
Tailored Hybrid Approach		
<p>Our hybrid approach ensures that while the project <b>benefits from the structured clarity of waterfall</b>, it also retains the <b>adaptability and client-centric focus of agile</b>. This duality allows us to deliver projects with greater efficiency, responding to new insights and changes without sacrificing control or clarity. The result is a delivery model that is robust, flexible, and oriented towards achieving project goals effectively.</p>		

To deliver this modified agile methodology, our PMP-certified project managers collaborate with Scrum and Scaled Agile Framework (SAFe) certified professionals. This team structure allows for quick adaptation to change, fostering collaboration and continuous improvement through regular feedback. The leadership is designed to maintain a balance between strict project management discipline and the dynamic, adaptive approach of agile methodologies. This ensures that the

---

project not only stays on course to meet its milestones but also adapts seamlessly to changing requirements, ultimately achieving its objectives with efficiency.

### 6.3 Expected Level of Client Engagement

The State will be responsible for having an engaged Sponsor and Project Owner, in addition to making available technical and subject matter experts as well as business users and stakeholders. Clango expects that clients allocate adequate internal resources, including team members who will work alongside Clango's team, to support various project phases (*see project team structure below*). The availability of these resources, as per the agreed upon project schedule, is necessary to avoid delays. Additionally, we expect that our clients will help facilitate access to key stakeholders and decision-makers when required for interviews, meetings, or to provide specific insights. This ensures a comprehensive understanding and alignment across all levels of the organization. Lastly, it is our expectation that clients do their best to adhere to the agreed-upon timelines for reviews, meetings, and delivery of required information. Two of the most critical aspects of client engagement include:

- **Designated Point of Contact:**

Assigning a dedicated point of contact for the Clango team to streamline communication and decision-making processes is essential. This individual should have the authority and knowledge to provide insights and make decisions pertinent to the project.

- **Timely Feedback and Decision Making:**

Prompt feedback and decision-making from the client's side on recommendations and findings presented by Clango are crucial to maintaining project momentum. Delays in these areas can impact the project timeline and outcomes.

### 6.4 Data Prep and Process Reviews

For successful execution of our IAM implementation projects, we want to ensure that our clients are well-prepared, and expectations related to data preparation and process reviews between the two parties are mutually understood. This clarity ensures that we are in alignment, paving the way for an efficient and effective engagement. Clango typically expects the following:

- **Data Availability:**

Clients should provide complete access to relevant data that Clango's team needs for analysis. This includes, but is not limited to, existing IAM policies, user access logs, system architecture diagrams, and current IAM tool configurations.

- **Data Accuracy and Integrity:**

The data provided should be current, accurate, and comprehensive. This ensures that the team can make well-informed decisions and recommendations. Any known issues or inconsistencies in the data should be communicated upfront.

---

- **Collaborative Review of Existing Processes:**

Clients should be prepared to engage in detailed discussions regarding their current IAM processes and procedures. Participation in process review sessions, bringing in key personnel who understand the existing workflows and challenges, is essential.

- **Readiness for Solution-Fit Analysis:**

Clients should be open to an objective assessment of their current IAM state. This involves acknowledging potential gaps or inefficiencies in their existing processes and technologies and capabilities of our proposed solution. Transparency in discussing these aspects is critical for identifying areas of improvement and ensuring specific solution fit and requirements coverage.

- **Preparation for Change Management:**

Clients should be ready to consider recommendations for change management, understanding that improvements might require adjustments to current practices. An open mindset toward adapting new strategies and technologies is fundamental for the project's success.

## **6.5 Project Team Structure**

According to Gartner, “Identity Governance and Administration (IGA) is an essential, but complex, Identity and Access Management (IAM) discipline”, an opinion that Clango shares and one that underscores the essential need for strong partnership between the customer, vendor, and integrator in the delivery, installation, and operation of any IAM/IGA solution.

At the start of every engagement, Clango believes that success is predicated on establishing a capable and engaged Integrated Project Team (IPT). The typical IPT, pictured below, will be led on the Clango side by our proposed Project Manager (PM) with support from key personnel (*see resumes in section below for proposed project personnel*) in the roles of Business Analyst, IAM Lead Architect, IAM Engineers, SMEs, and Testers. Clients are responsible for having an engaged Executive Sponsor/Business Lead, in addition to making available technical and subject matter experts.

INTEGRATED PROJECT TEAM	
CLANGO TEAM ROLES	STATE OF WEST VIRGINIA ROLES
<p><b>Project Manager</b></p> <ul style="list-style-type: none"> <li>• Extensive experience on IAM/IGA projects.</li> <li>• Provides total project management.</li> <li>• Manages resources, drives task execution, resolves issues, and escalates blockers.</li> <li>• Primary escalation point for Clango.</li> </ul> <p><b>Business Analyst</b></p> <ul style="list-style-type: none"> <li>• Experience with IAM/IGA solutions and best practices.</li> <li>• Document current state and future requirements.</li> <li>• Prepares use cases and business processes.</li> </ul> <p><b>IAM Lead / Architect</b></p> <ul style="list-style-type: none"> <li>• Broad IAM/IGA experience.</li> <li>• Technical and functional IAM expert.</li> <li>• Drives use case solutioning based on requirements.</li> <li>• Specify solution configuration and lead engineering team.</li> </ul> <p><b>IAM Engineers / SMEs</b></p> <ul style="list-style-type: none"> <li>• IAM/IGA solution implementation experience with product for similar customers.</li> <li>• Performs solution configuration / develops integrations.</li> <li>• Assists with system reviews and review of existing artifacts.</li> </ul> <p><b>Tester</b></p> <ul style="list-style-type: none"> <li>• IAM/IGA solution implementation experience</li> <li>• Experience developing formal software test plans and test cases.</li> <li>• Drives testing activities and liaison with client UAT team.</li> </ul>	<p><b>Executive Sponsor/ Business Lead</b></p> <ul style="list-style-type: none"> <li>• Understands the business process, has executive direction, and can make critical IAM (identity and access management) decisions.</li> <li>• Ownership of IAM platform.</li> </ul> <p><b>Project Manager</b></p> <ul style="list-style-type: none"> <li>• Align and assign resources, ensures issue resolution on the client side, and acts as the primary escalation point.</li> </ul> <p><b>Technical Lead</b></p> <ul style="list-style-type: none"> <li>• Broad experience with various technical subjects as well as skills in the areas of infrastructure design, requirements and gap analysis, and preferably prior implementation experience.</li> </ul> <p><b>Technical Team / SMEs</b></p> <ul style="list-style-type: none"> <li>• Ensures solution conforms to the organization's architecture, standards, and meets enterprise needs.</li> <li>• Intimate knowledge of existing IAM system and current processes / use cases.</li> </ul> <p><b>User Acceptance Testers</b></p> <ul style="list-style-type: none"> <li>• Personnel who will be testing the solution to ensure the project implementation meets business requirements.</li> </ul>

## 6.6 Proposed Implementation Plan

The following project implementation plan is based on the requirements as currently understood and the best-practice implementation methodology that we have used to deliver Identity Management solutions for similar client engagements. For each phase of the project, we provide activities and the related tasks, along with the prospective deliverables, and the Clango team activities as well as the State's responsibilities. At the start of the project, we will refine the implementation plan based on further discovery and requirements gathering and generate the baseline project schedule with milestones.

### 6.6.1 Phase 1: Project Kickoff, Discovery & Workshops

Activity	Tasks	Deliverables	Clango Activities	State of West Virginia Activity List
<b>Project Planning and Kickoff</b>	Project Kickoff	<ul style="list-style-type: none"> <li>• Project Management Plan</li> <li>• Kickoff Presentation</li> <li>• Schedule recurring project meetings</li> </ul>	<ul style="list-style-type: none"> <li>• Create project management plan</li> <li>• Schedule and hold kickoff</li> <li>• Schedule recurring project meetings</li> </ul>	<ul style="list-style-type: none"> <li>• Identify stakeholders and contacts</li> <li>• Participate in project kickoff</li> <li>• Onboard team members to Customer network</li> </ul>
<b>Discovery, Requirements Definition &amp; Architecture Workshops</b>	Strategic Architecture and Requirements Workshop	<ul style="list-style-type: none"> <li>• Strategic Requirements Gathering</li> <li>• Identify and Document Requirements</li> <li>• Identify and Document MFA Use Cases</li> </ul>	<ul style="list-style-type: none"> <li>• Lead strategic architecture workshops</li> <li>• Present CyberArk Identity Best Practices</li> <li>• Discover and review MFA options</li> <li>• Discover and review Application requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Participate in Strategic Architecture and Requirements workshops</li> <li>• Review CyberArk Best Practices</li> <li>• Review requirements</li> </ul>

### Phase 2: CyberArk Identity Setup & Microsoft Integrations

Activity	Tasks	Deliverables	Clango Activities	State of West Virginia Activity List
<b>Foundational Configuration</b>	CyberArk Identity Configuration	<ul style="list-style-type: none"> <li>• Functional CyberArk Development tenant</li> </ul>	<ul style="list-style-type: none"> <li>• Configure CyberArk Identity Dev tenant</li> </ul>	

	Migrate existing user base into CyberArk Identity	<ul style="list-style-type: none"> <li>• Users populated in CyberArk Identity Store</li> </ul>	<ul style="list-style-type: none"> <li>• Review existing LDAP Store</li> <li>• Ensure Attribute Mapping</li> <li>• Script Migration</li> <li>• Validate</li> <li>• Remediate any found issues</li> </ul>	<ul style="list-style-type: none"> <li>• Validate Attribute Mapping</li> <li>• Validate Migration</li> </ul>
	MFA Factor Setup	<ul style="list-style-type: none"> <li>• MFA Factors configured</li> </ul>	<ul style="list-style-type: none"> <li>• Configure MFA Factors in CyberArk Identity</li> </ul>	<ul style="list-style-type: none"> <li>• Attend configuration session to validate MFA factors meet use cases</li> </ul>
	SSO Setup	<ul style="list-style-type: none"> <li>• Create base SSO Configuration</li> </ul>	<ul style="list-style-type: none"> <li>• Create base SSO Configuration</li> </ul>	<ul style="list-style-type: none"> <li>• Attend configuration session to validate SSO meets use cases</li> </ul>
	Active Directory	<ul style="list-style-type: none"> <li>• Enable MFA for AD</li> </ul>	<ul style="list-style-type: none"> <li>• Configure MFA for AD</li> </ul>	<ul style="list-style-type: none"> <li>• Provide resources needed to setup MFA or provide appropriate access</li> </ul>
<b>Testing and Validation</b>	Complete testing of all configured objects	<ul style="list-style-type: none"> <li>• Validate current functionality</li> </ul>	<ul style="list-style-type: none"> <li>• Perform testing</li> </ul>	
	Develop a test plan that comprehensively covers requirements and defines success criteria	<ul style="list-style-type: none"> <li>• Document test plan for CyberArk Identity, AD</li> </ul>	<ul style="list-style-type: none"> <li>• Prepare test cases for Customer testing activities</li> </ul>	<ul style="list-style-type: none"> <li>• Review proposed test cases</li> </ul>
	Support UAT, including monitoring, feedback and issue resolution	<ul style="list-style-type: none"> <li>• System ready for end user rollout</li> </ul>	<ul style="list-style-type: none"> <li>• Support Customer UAT Testing</li> </ul>	<ul style="list-style-type: none"> <li>• Complete UAT testing</li> <li>• Provide timely feedback</li> </ul>



		<ul style="list-style-type: none"> <li>• Testing Monitoring</li> <li>• Testing Issue resolution</li> </ul>	<ul style="list-style-type: none"> <li>• Remediate any found issues</li> </ul>	concerning needs and issues
<b>Documentation of configuration for Change Management</b>	Prepare documentation to Customer Standards	<ul style="list-style-type: none"> <li>• Documentation artifacts required to obtain approval to rollout to end users</li> </ul>	<ul style="list-style-type: none"> <li>• Create migration documentation in Customer approved format</li> </ul>	<ul style="list-style-type: none"> <li>• Provide format and presentation requirements</li> </ul>
<b>Training For Support Team(s)</b>	Conduct training with Customer Support Team(s)	<ul style="list-style-type: none"> <li>• Support Teams attend training and feel prepared to take on support of CyberArk Identity</li> <li>• Create runbook of CyberArk Identity configuration</li> </ul>	<ul style="list-style-type: none"> <li>• Provide training</li> </ul>	<ul style="list-style-type: none"> <li>• Appropriate team(s) attend training</li> </ul>
<b>Org change for end users</b>	Create material to support org change for end users	<ul style="list-style-type: none"> <li>• Appropriate processes, procedures &amp; run books to support end users provided</li> </ul>	<ul style="list-style-type: none"> <li>• Create and deliver all material necessary to support org change for end users</li> <li>• Make revisions as Customer sees fit</li> </ul>	<ul style="list-style-type: none"> <li>• Review and provide feedback</li> </ul>
<b>Preparation and Go Live for Phase 2</b>	Enable MFA, SSO for AD	<ul style="list-style-type: none"> <li>• System in Production for MFA, SSO</li> </ul>	<ul style="list-style-type: none"> <li>• Execute go live plan in agreed upon collaboration with Customer</li> </ul>	<ul style="list-style-type: none"> <li>• Collaborate with Clango on go live</li> </ul>

### 6.6.2 Phase 3: Application Setup & Configuration

Activity	Tasks	Deliverables	Clango Activities	State of West Virginia Activity List
<b>Application Setup</b>	Configure up to five Marketplace applications identified during discovery	<ul style="list-style-type: none"> <li>• MFA enabled for each application</li> </ul>	<ul style="list-style-type: none"> <li>• Configure MFA for applications</li> </ul>	<ul style="list-style-type: none"> <li>• Provide resources needed to setup MFA or provide appropriate access</li> </ul>
<b>Testing and Validation</b>	Complete testing of all configured objects	<ul style="list-style-type: none"> <li>• Validate current functionality</li> </ul>	<ul style="list-style-type: none"> <li>• Perform testing</li> </ul>	
	Develop a test plan that comprehensively covers requirements and defines success criteria	<ul style="list-style-type: none"> <li>• Document test plan for configured applications</li> </ul>	<ul style="list-style-type: none"> <li>• Prepare test cases for Customer testing activities</li> </ul>	<ul style="list-style-type: none"> <li>• Review proposed test cases</li> </ul>
	Support UAT, including monitoring, feedback and issue resolution	<ul style="list-style-type: none"> <li>• System ready for end user rollout</li> <li>• Testing Monitoring</li> <li>• Testing Issue resolution</li> </ul>	<ul style="list-style-type: none"> <li>• Support the Customer with UAT Testing</li> <li>• Remediate any found issues</li> </ul>	<ul style="list-style-type: none"> <li>• Complete UAT testing</li> <li>• Provide timely feedback concerning needs and issues</li> </ul>
<b>Documentation of configuration for Change Management</b>	Prepare documentation to Customer Standards	<ul style="list-style-type: none"> <li>• Documentation artifacts required to obtain approval to rollout to end users</li> </ul>	<ul style="list-style-type: none"> <li>• Create migration documentation in Customer approved format</li> </ul>	<ul style="list-style-type: none"> <li>• Provide format and presentation requirements</li> </ul>
<b>Training For Support Team(s)</b>	Conduct training with Customer Support Team(s)	<ul style="list-style-type: none"> <li>• Support Teams attend training and feel prepared to take on support of CyberArk Identity</li> <li>• Create runbook of CyberArk Identity configuration</li> </ul>	<ul style="list-style-type: none"> <li>• Provide training</li> </ul>	<ul style="list-style-type: none"> <li>• Appropriate team(s) attend training</li> </ul>

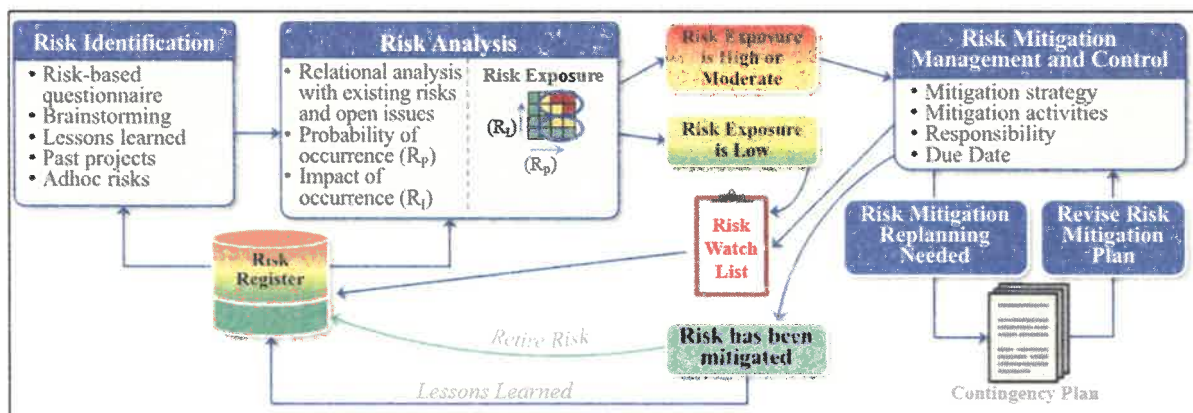
<b>Org change for end users</b>	Create material to support org change for end users	<ul style="list-style-type: none"> <li>• Appropriate processes, procedures &amp; run books to support end users provided</li> </ul>	<ul style="list-style-type: none"> <li>• Create and deliver all material necessary to support org change for end users</li> <li>• Make revisions as the Customer sees fit</li> </ul>	<ul style="list-style-type: none"> <li>• Review and provide feedback</li> </ul>
<b>Preparation and Go Live for Phase 3</b>	Enable MFA for applications	<ul style="list-style-type: none"> <li>• MFA live for applications in CyberArk Identity</li> </ul>	<ul style="list-style-type: none"> <li>• Execute go live plan in agreed upon collaboration with the Customer</li> </ul>	<ul style="list-style-type: none"> <li>• Collaborate with Clango on go live</li> </ul>

### 6.6.3 Proposed Project Schedule

	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15	Week 16
Phase 1																
Phase 2																
Phase 3																

## 6.7 Managing Implementation Risks

Clango’s approach to the identification, assessment and mitigation of risks associated with meeting the requirements of Identity Management Implementation projects uses the PMBOK®-based process (described in the figure below) to proactively identify and eliminate potential problems that could impact quality within the scope of our services. Our risk management process includes viewing each task area, events, and deliverables identified within the scope of work and integrating task-level risk management into our quality management procedures. Our proven methodology addresses all task activities, and our streamlined management structure facilitates agility through monitoring and continuous communications with client leadership and stakeholders. This enables us to adapt quickly to identify and mitigate potential risks.



Once a risk has been identified and assessed, we discuss solution options with our client, involving appropriate stakeholders for their input. We then implement risk prioritization and controls, using proven, approved checklists and processes. Our risk strategy includes evaluating multiple options to manage and mitigate a risk to an acceptable level. We identify resources and potential related expenses and recommend how risk mitigation(s) and/or contingencies will be implemented. We obtain approval from your management before putting any plan into action. Our goal is to record and manage all operational and program risks and impacts to your organization and stakeholders to reduce unnecessary costs, security risks, and project delays.

## 6.8 Mitigating Common IAM Implementation Risks

Throughout our implementations, we communicate and consult with stakeholders to ensure that the following common risks associated with Identity Management implementation projects are managed to ensure project objectives and stakeholders’ expectations are achieved.

<b><i>Project Management and Governance Issues</i></b>	
<b>Risk</b>	In an IAM implementation, this pertains to the lack of clear leadership, poorly defined objectives, and inadequate stakeholder engagement. These issues can result in misaligned IAM goals with business requirements.
<b>Mitigation</b>	On all engagements, Clango establishes a robust governance framework with clear roles and responsibilities and our proven delivery approach engages stakeholders through regular communication to ensure that project goals are aligned with the strategic objectives of the organization.
<b><i>Budget Overruns</i></b>	
<b>Risk</b>	IAM projects can incur additional costs due to unforeseen complexities and scope changes, leading to budget overruns.
<b>Mitigation</b>	Clango conducts thorough planning and risk assessments to accommodate potential financial contingencies and implements strict scope management and change control processes.
<b><i>Data Quality Issues</i></b>	
<b>Risk</b>	An IAM system is only as good as the data it manages. Inconsistent or inaccurate data can compromise security and user experience.
<b>Mitigation</b>	We prioritize data cleaning and establish ongoing data quality management practices and use data validation tools to ensure accuracy and consistency.
<b><i>Integration Challenges</i></b>	
<b>Risk</b>	Integrating the IAM solution with existing systems can be complex and may face technical and compatibility issues.
<b>Mitigation</b>	We develop a comprehensive integration strategy that includes evaluation of existing systems, a phased integration approach, and thorough testing.
<b><i>SaaS Product Update Frequency</i></b>	
<b>Risk</b>	The rapid update cycles of SaaS products can conflict with the stability needed in IAM systems.
<b>Mitigation</b>	Clango works closely with SaaS vendors to understand the product update roadmap and prepare the client's IAM environment for updates. We implement robust testing procedures for updates in a staging environment before production deployment.
<b><i>User Adoption</i></b>	
<b>Risk</b>	Resistance to change can hinder the successful implementation of IAM systems.

<b>Mitigation</b>	Clango collaborates with our clients to facilitate and manage detailed change management strategies, including user training programs and a support structure to assist users during the transition.
<b>Regulatory Compliance</b>	
<b>Risk</b>	IAM implementations must adhere to various regulations, which can be challenging due to the evolving nature of compliance requirements.
<b>Mitigation</b>	Clango's team continuously monitors regulatory changes and adjusts the IAM policies accordingly and we conduct regular compliance audits.

## 6.9 Quality Control Methods

Clango's quality control methods define monitoring procedures that identify impending variances before they impact quality, cost, or schedule performance and prevent issues from occurring. For all implementation projects, at a minimum, these procedures include:

- Clearly defined quality requirements, standards, and procedures to be used for all project tasks and delivery of services to include defining all methods, frequency, and the metrics to be collected including high quality technical performance, adherence to schedule, adherence to budget, staffing and others as mutually agreed upon by Team Clango and the State's leadership.
- QC frequency standards (e.g., performed at every phase of development to ensure deliverables and outputs meet the defined requirements and standards).
- Quality Assurance (QA) review standards (e.g., verify defined processes and procedures are being followed and opportunities for improvement are identified).
- Continual improvement review (e.g., identify ways in which services and/or quality can be improved).
- Provide a repository of quality documentation available to appropriate stakeholders through collaboration and information sharing tools, such as MS Teams and SharePoint.

We use a variety of internal tools and processes to verify that work products follow standards, meet requirements and are of the highest caliber. The following are examples of processes and tools employed to manage quality:

- **Peer Reviews:** Peer reviews are performed regularly for client deliverables to verify content, coverage, adequacy, accuracy, and adherence to established processes. We use peer reviews on code, documentation, testing, and formal project artifact deliverables such as FRDs, RTMs, Design Documents, written Business Practices, Training Material, and Organizational Change Management communications.

- **Document Templates:** Client documentation is developed using client-specified templates (when required). If the State of West Virginia does not require specific templates or formats for deliverables, we will apply templates from our library of standardized templates that we have developed and refined over hundreds of Identity Management implementation projects.
- **Deliverable Preparation and Acceptance:** For each deliverable, we prepare a draft version to be reviewed with the client Project Manager and/or Project Management Team, as applicable, and as early as possible. In the final stage of preparing a deliverable, peer reviews are conducted to provide feedback on the deliverable and identify and correct any noncompliant items and incorporate the State’s feedback. Clango’s PM (and Lead Architect) will deem the deliverable to be ready, the reviews and the final document will be stored on the designated project portal (i.e., SharePoint or Teams Site) and within the identified project repository.

### 6.10 Resolution of Blockers and Implementation Activities

In delivering Identity Management (IAM) projects, Clango adopts a structured approach to efficiently resolve blockers and work activity conflicts, especially considering the compact timelines of the engagements. The key elements (in the table below) describe our approach to ensure projects stay on track and meet the objectives within the stipulated timeframe.

<b>Early Identification and Analysis:</b>	<ul style="list-style-type: none"> <li>● Proactively identify potential blockers and conflicts at the beginning of the project through a risk assessment.</li> <li>● Continuously monitor for any emerging issues during the project.</li> </ul>
<b>Open Communication Channels:</b>	<ul style="list-style-type: none"> <li>● Establish clear, open lines of communication with all stakeholders and team members.</li> <li>● Encourage prompt reporting of any challenges or conflicts that arise.</li> </ul>
<b>Prioritization and Triage:</b>	<ul style="list-style-type: none"> <li>● Prioritize issues based on their impact on the project timeline and goals.</li> <li>● Apply a triage system to address the most critical issues first, while balancing other ongoing tasks.</li> </ul>
<b>Collaborative Problem-Solving:</b>	<ul style="list-style-type: none"> <li>● Engage relevant stakeholders in brainstorming sessions to find mutually agreeable solutions.</li> <li>● Foster a collaborative environment where all voices are heard, and different perspectives are considered.</li> </ul>

<b>Adaptive Project Management:</b>	<ul style="list-style-type: none"> <li>• Utilize agile methodologies to remain flexible and adapt to changing circumstances.</li> <li>• Implement an iterative process that allows for continuous evaluation and adjustment of the project plan.</li> </ul>
<b>Escalation Procedures:</b>	<ul style="list-style-type: none"> <li>• Clearly define escalation paths for issues beyond the scope of the immediate team.</li> <li>• Ensure timely escalation to senior management, when necessary, to prevent any stagnation.</li> </ul>
<b>Regular Status Updates:</b>	<ul style="list-style-type: none"> <li>• Provide regular updates to all stakeholders about the progress of the project, including how blockers and conflicts are being handled.</li> <li>• Maintain transparency throughout the process to build trust and manage expectations.</li> </ul>

## 6.11 Change Management and Communications

The development of an Identity Management program's communications and change management process is a crucial aspect of ensuring its continued success. Clango's team of IAM advisors leverages their extensive IAM implementation experience when designing and developing change management, communication, and training programs to create impactful materials tailored for each department and stakeholder to secure organizational buy-in from all personnel.

The Key aspects and elements of our approach for developing IAM Program Communications and Change Management materials includes:

- Identify the key messages and objectives for the IAM program that need to be communicated across the organization.
- Develop tailored content that resonates with the specific interests and responsibilities of each audience segment.
- Create a narrative that explains the IAM program's benefits, its impact on individual roles, and its significance in enhancing organizational security.
- Incorporate industry best practices and Clango's proven methodologies in the content to establish credibility and trust.
- Highlight success stories and case studies from Clango's vast experience to demonstrate the practical benefits of the IAM program.
- Design the materials in engaging formats such as presentations, infographics, and interactive sessions that encourage active participation.



- 
- Utilize visual aids and real-world scenarios to make the information more relatable and easier to understand.
  - Ensure that roadshow sessions are interactive, allowing for Q&A, discussions, and feedback to address any concerns and clarify doubts.
  - Use simple, jargon-free language to explain technical aspects, ensuring clarity and comprehension.
  - Establish a feedback loop to gather insights from employees on the materials presented.
  - Use this feedback to refine the approach, content, and delivery of the IAM program’s internal marketing efforts.
  - Develop a plan for ongoing communication and updates about the IAM program to keep the momentum and engagement alive.
  - Implement metrics to evaluate the effectiveness of the internal marketing/roadshow efforts in terms of employee engagement and understanding.

## 6.12 Training

As part of the implementation, Clango will develop and provide training for administrators and users for features and functionality related to the CyberArk Identity Solution. Training will focus on ensuring that users of the system understand:

- The role of CyberArk Identity at the State
- Their role in using the CyberArk Identity system

The training delivery method may include online web conferences, train the trainer sessions, and training videos. Written training documentation will be tailored based on the stakeholder needs and complexity of features. Regardless of format, our team will ensure that the training is developed to capture core application functionality and that it is categorized and divided into logical modules, sessions, and training classes. Any lessons learned or recommended changes to the training program will also be incorporated.

We find that a combination of formal training and informal knowledge transfer proves very effective in enabling customers to be self-sufficient over the course of a project.

Finally, we provide written training documentation that can be used along with—or in addition to—the other techniques mentioned above. Some examples of written training documentation that Clango has used in past projects include user manuals, run books, quick reference guides, workflow documentation, and checklists for specific tasks. We will incorporate screenshots in the training documents to illustrate what is being described in the text.

Clango also recommends that customers review solution OEM training options to augment or add to our formal and informal training.

### 6.13 CyberArk OEM Support

CyberArk currently has over 3,000 employees worldwide, with approximately 10% of these employees focused exclusively on the CyberArk Identity product lines. After becoming a customer, the State will have access to standard technical support during business hours as part of the SaaS subscription.

A dedicated Customer Service Team along with the account manager will make sure the performance and usage of the software is satisfactory and provide guidance and advice on a regular basis. The State’s customer success manager will be a named resource that will have the required technical background and knowledge.

Apart from a robust technical support organization, customers can leverage CyberArk’s Technical Community that contains more than 3,000 self-service resources with step-by-step instructions to install and configure CyberArk’s solutions and how-to videos to online documentation are available. In addition, a vast community of users also engage and collaborate providing more than 9,000 questions and 35,000 answers. The Technical Community is a one-stop shop for CyberArk resources available for customers and partners and a great place to get product questions answered fast.

## 7 Experience and Qualifications

### 7.1 Corporate Information Summary

Clango, Inc. Corporate Information Summary			
<b>Year Business Established</b>	1993		
<b>Type of Ownership</b>	Minority-Owned Private, Maryland S-Corporation		
<b>Business Size</b>	Small		
<b>Authorized Representatives</b>	<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;">                     Duane Graham, CEO                      2107 Wilson Blvd, Suite 250                      Arlington, VA 22201                      Phone: 571-483-2720 (direct)  <a href="mailto:dgraham@clango.com">dgraham@clango.com</a> </td> <td style="width: 50%; vertical-align: top;">                     Patrick McGeehan, VP of Service Delivery                      2107 Wilson Blvd, Suite 250                      Arlington, VA 22201                      Phone: 571-483-2727 (direct)  <a href="mailto:pmcgeehan@clango.com">pmcgeehan@clango.com</a> </td> </tr> </table>	Duane Graham, CEO 2107 Wilson Blvd, Suite 250 Arlington, VA 22201 Phone: 571-483-2720 (direct) <a href="mailto:dgraham@clango.com">dgraham@clango.com</a>	Patrick McGeehan, VP of Service Delivery 2107 Wilson Blvd, Suite 250 Arlington, VA 22201 Phone: 571-483-2727 (direct) <a href="mailto:pmcgeehan@clango.com">pmcgeehan@clango.com</a>
Duane Graham, CEO 2107 Wilson Blvd, Suite 250 Arlington, VA 22201 Phone: 571-483-2720 (direct) <a href="mailto:dgraham@clango.com">dgraham@clango.com</a>	Patrick McGeehan, VP of Service Delivery 2107 Wilson Blvd, Suite 250 Arlington, VA 22201 Phone: 571-483-2727 (direct) <a href="mailto:pmcgeehan@clango.com">pmcgeehan@clango.com</a>		

<b>Office Locations/Addresses</b>	<u>Headquarters:</u> 2107 Wilson Blvd., Suite 250 Arlington, VA 22201 Phone: 703-534-3309	<u>Minneapolis, MN:</u> 8011 34 <sup>th</sup> Ave. South, Suite 350 Bloomington, MN 55425 Phone: 651-631-3144	<u>Jonestown, PA:</u> 319 Washington St., Suite 340 Johnstown, PA 15901 Phone: 814-262-8629
<b>Years Providing Identity Security Services</b>	16+		
<b>Employees Solely Dedicated to Identity Security (IAM &amp; PAM)</b>	90+		
<b>Website</b>	www.clango.com		

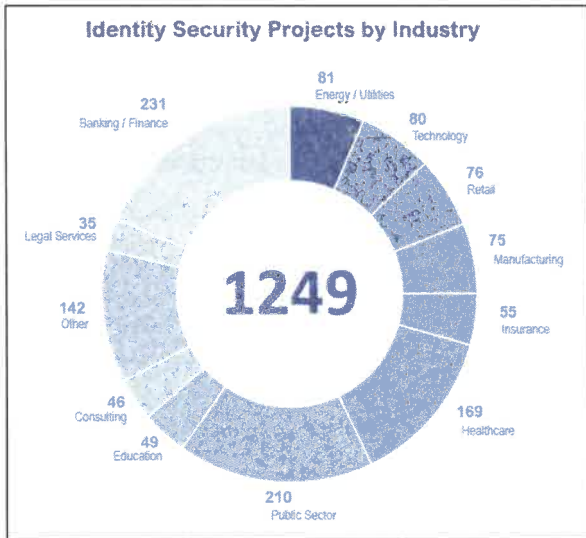
## 7.2 Clango Corporate Qualifications

Clango is one of CyberArk’s fastest growing, agile, and qualified small business Advanced Professional Services partners and authorized resellers. For the past 8 years, Clango has made substantial investments in hiring, training, and developing a team of industry-leading identity security engineers focused on implementing CyberArk’s portfolio of solutions. What began with a single implementation of CyberArk at the end of 2015 has grown to a current team of more than 45 full-time CyberArk Certified Delivery Engineers (CCDEs). Our CyberArk service delivery team is designed for rapid deployment, with a goal of maintaining our services backlog at three weeks or less – from contract award to project initiation (boots on the ground). As a trusted CyberArk professional services partner and value-added reseller, our engagements cover the full breadth of services, from implementation to longer-term undertakings that focus on helping customers mature their identity security programs (IAM/IGA/PAM) to achieve long-lasting success.



### 7.2.1 Relevant Experience – Public Sector

Clango has a rich history of executing successful engineering, deployment, and lifecycle sustainment projects at both the state and local level.



At the state government level, we are currently assisting the state of Illinois to implement a new Identity and Access Management solution. Additionally, we have completed multiple projects with the state of Minnesota, and have also worked directly with Virginia, Connecticut, Indiana, Maryland, and Texas. Our municipal customers include the City of Chicago, Chester County (PA), Clark County (WA), Hillsborough County (FL), Highlands County (FL), Ramsey County (MN), Fulton County (GA), and Will County (IL). In addition to our strong presence in the State & Local market, we have also achieved remarkable success within the broader Public Sector vertical. Our track record for delivering

successful projects includes more than 35 federal agencies and departments.

In addition to our prominent public sector engagements, our portfolio includes a diverse range of commercial organizations spanning multiple market verticals. This includes more than 50 Fortune 500 companies, retail conglomerates, healthcare entities, insurance firms, transportation, manufacturing, regulated utilities, agricultural co-ops, multinational banks, multibillion-dollar investment firms, and renowned technology companies. The subsequent experience write-ups showcase Clango's proficiency in delivering the services requested and required in the RFP.

### DELIVERY EXCELLENCE IS IN OUR DNA

 **1200+**  
Successful projects across all verticals

 **200**  
Identity Security Engagements in 2023

 **150**  
CyberArk & SailPoint Certifications

 **100%**  
Of our engineers possess an IAM certification

 **10+**  
Identity-Centric Products / Tools

 **1000s**  
Of Automated Business Processes



**CYBERARK**  
CyberArk Growth Partner of the Year AND Services Delivery Partner of the Year

**SailPoint**  
Delivery Admiral

**Delinea**   **Microsoft**   **ORACLE**   **RSA**

**ForgeRock**   **auth0**   **okta**

Clango listed in Gartner Hype Cycle™ for IAM Technologies as an IAM Managed Service Vendor

**Project-Based Services**  
**Advisory Services**  
**Managed Services**



Clango has served hundreds of customers in the identity security space in all types of engagements, including advisory, installation, upgrades, migration, and operation & maintenance with CyberArk products.

Use or disclosure of data contained on this page is subject to restrictions contained in the Request for Confidentiality statement of this document.

Page 40

### 7.3 Qualifications of Staff

Currently, Clango employs more than 110 people, of which 90+ are highly trained and experienced client-facing project managers, identity security advisors, engineers, architects, and developers who make up our delivery teams that are solely focused on identity security. Our team members hold several industry and cybersecurity-specific certifications, including: CISSP, CIGE, CEH, CISM, CISA, and CIAM. Our project managers and support staff hold PMP, ITIL V2/V3, and Scrum Master certifications. Our engineers validate and augment their vendor-specific training and certifications with additional credentials, including Security+ and Network+, as well as IAM and PAM-specific certifications. In total, Clango’s identity security professionals hold more than 150 industry and product certifications and are cross-trained and certified on numerous technologies, including CyberArk, SailPoint, Omada, RSA, Oracle, Delinea (formerly Thycotic), and Okta.

For any given project, we have the capability to provide expert advisors, identity security strategists, identity architects, implementation specialists, developers, and network engineers for both cloud and on-prem solutions.

All our engineers are CyberArk-certified at least at the Sentry Level, with five members of our staff being Guardian Certified (CyberArk’s highest certification level). Our team members undergo a rigorous training program that includes multiple hands-on trainings, labs, tech challenges, and on-the-job shadowing with real customers. Our engineers are adept at solving difficult problems and designing robust solutions to improve the security of an organization’s most critical accounts, including configuring CyberArk to assist in auditing and controls compliance for SOX, PCI/DSS, GDPR, PII, HIPAA/HITECH, NIST SP 800-43, and many other security frameworks. All of our team members are cross trained in multiple technologies, hold multiple certifications, and have an average of seven years of experience in the industry.

 <p><b>LEVEL ONE: TRUSTEE</b></p> <p>The holder of this certificate has proven their basic knowledge of the use of privileged access in cyber security, as well as an understanding of the CyberArk solutions.</p>	 <p><b>LEVEL TWO: DEFENDER</b></p> <p>The holder of this certification has proven their theoretical and hands on expertise in the daily maintenance and operation tasks of the Privileged Access Security Solution.</p>
 <p><b>LEVEL THREE: SENTRY</b></p> <p>The holder of Sentry certification has proven their skills, both theoretical and hands on, with the deployment and configuration of the CyberArk solution.</p>	 <p><b>LEVEL FOUR: GUARDIAN</b></p> <p>Holders of this certification have proven their advanced skills with the various CyberArk solutions and their ability to configure organizations' architecture with privileged access security strategy.</p>

Clango has staff distributed across our Arlington, VA, Minneapolis, MN, and Johnstown, PA offices, as well as several engineers who are remote employees located throughout the country (We have engineers in all time zones). Our organization is structured to promote collaboration across these different geographies to ensure our clients’ identity projects are successful. We prioritize employees’ project-skill fit over geographical location to ensure our clients get the right team for the job.

## 7.4 Proposed Project Personnel (Resumes)

Our proposed project manager and senior technical resources for this project represent Clango’s senior-most identity security implementation team members. As project manager, Thomas Yee is an accomplished PM with a PMP certification and more than 15 years of extensive experience guiding identity security and cybersecurity programs and implementations across the public sector, financial services, and healthcare sectors. In senior technical roles, both Dan Ross and Son Pham hold CyberArk’s highest certification level (Guardian) and have a total of **more than 50 years’ experience between them delivering customer IT solutions**. Resumes for Thomas, Dan and Son are provided below. Upon award, Clango will assign additional team personnel from our identity security practice to the delivery team.

### 7.4.1 Thomas Yee (Project Manager)

<b>Resource: Thomas Yee</b>	
<b>Project Role:</b> Project Manager	<b>Company:</b> Clango Employee 2021-Present <b>Years of Experience:</b> 15+
<b>Summary</b>	
Thomas Yee is a PMP-certified Project Manager with more than 15 years of experience serving a variety of clients in the public sector, financial services, and healthcare markets. He has managed numerous infrastructure upgrades, integration efforts, and support projects, as well as managing Cybersecurity Program portfolios of 30+ projects.	
<b>Systems Experience</b>	
<ul style="list-style-type: none"> <li>• COTS: Visio, MS Project, Tableau</li> <li>• Programming: C++, SQL, HTML</li> <li>• Databases: Oracle, Microsoft SQL Server</li> <li>• Security: SailPoint IIQ/IDN, Thycotic (Delinea), CybeReason</li> <li>• Operating Systems: Windows (all versions), Linux</li> </ul>	
<b>Certifications</b>	
<ul style="list-style-type: none"> <li>• Project Management Professional (PMP)</li> </ul>	
<b>Relevant Experience: Clango, Inc.</b>	
<b>Project Manager</b> <b>Bank of Montreal</b> <b>Project Manager / Release Manager</b>	<b>Dec. 2021 – Present</b>
Served as Project Manager / Release manager and project management support for implementation of SailPoint IIQ at large financial institution. Project had high C-suite visibility, rapidly changing scope, and tight deadline.	
<ul style="list-style-type: none"> <li>• Coordinating QA and development teams comprised of two external partners and internal resources</li> <li>• Focused on week-to-week releases and overall go-live planning (including data reconciliation, new process documentation, infrastructure upgrades, and companywide communications)</li> <li>• Served as release manager for supporting high priority upgrades and development integration</li> <li>• Worked as liaison between the technical teams and the business to develop core product features</li> <li>• Advises and supports Clango engineering and advisory resources and provides escalation services to the Client</li> </ul>	

**Resource: Thomas Yee**

- Coordinates disparate SailPoint Engineer and Advisory Work Efforts
- Coordinates disparate CyberArk Engineer and Advisory Work Efforts
- Coordinates follow-on DevOps efforts around CyberArk and SailPoint automation and the Embark Deployment, including but not limited to Ansible development efforts

**Relevant Past Experience: Cerner Corporation*****Cybersecurity Program Manager*****Aug. 2019 – Dec. 2021**

Thomas's responsibilities and accomplishments included the following:

- IT Project manager with the Bear Institute at Children's National Hospital
- Project work including AWS data research platforms, interoperability, and clinical applications
- Organized and led project team resources for high profile system wide go-lives
- Program manager for overall cybersecurity portfolio (30+ projects)
  - Scoped tasks and resources with cross-functional IT teams to determine best case project prerequisites, overlap, and dependencies
  - Focused on organizational security strategy for overall program implementation
  - Led RFP efforts for Identity Access Management and Managed Security Service efforts
  - Coordinated between stakeholders' expectations, financial goals, and overall organization objectives to set the pace for the next 3 years of projects
  - Developed reporting for program metrics and utilized data to improve management processes

***Interoperability Project Manager*****June 2017 – Aug. 2019**

Thomas's responsibilities and accomplishments included the following:

- Client engagement specialist with focus on software implementation
- Healthcare Interoperability – consulting and strategy – including Commonwell, immunizations reporting and query, and open platform development (Ignite API)
- Coordinated multiple teams and clients for implementation of major regulatory requirements
- Team subject matter expert on FHIR API - SMART app implementation and development
  - Improved Ignite API implementation process; cut overall project duration by 35%
  - Served as team liaison for communication and coordination with Regulatory, Patient Engagement, Clinical Terminologist, and Software Development teams

**Relevant Past Experience: American Academy of Family Physicians*****Business Analyst*****2013 – 2017**

Thomas's responsibilities and accomplishments included the following:

- IT Project management, portfolio management, vendor relations
- Specialized in mobile application development and business intelligence
- Planned and oversaw organizational-wide rollout of BI tools for data-driven decision making
- Provided organizational training for new software and technology, including Tableau and JIRA
- Served as scrum leader for an Agile development team for web projects
- Investigated new IT solutions for web conferencing, e-commerce, and online education
- Revamped technology prioritization process to focus on ROI, MVP, and business need

<b>Resource: Thomas Yee</b>	
<b>Relevant Past Experience: Alliant TechSystems</b>	
<b>Manufacturing Project Engineer</b>	<b>2012-2013</b>
Thomas's responsibilities and accomplishments included the following:	
<ul style="list-style-type: none"> <li>• Investigated and assessed the validity and feasibility of upgrades to packaging area equipment.</li> <li>• Technical proposal preparation and root cause analysis of potential problems and solutions.</li> <li>• Coordinated efforts from disparate departments on a new unified packaging vision.</li> </ul>	
<b>Modeling Project Manager</b>	<b>2007-2012</b>
Thomas's responsibilities and accomplishments included the following:	
<ul style="list-style-type: none"> <li>• Managed a million-dollar project for a major government contract.</li> <li>• Led a research team that delivered industrial engineering support for Six Sigma, Lean, and modernization design initiatives; duties included resource planning and coordinating studies.</li> <li>• Provided cost-benefit analysis and reports that justified multimillion-dollar capital expenditure.</li> <li>• Rescued modeling project on the verge of cancellation &amp; completed it on time and under budget.</li> <li>• Created a process improvement procedure involving modeling and value stream mapping.</li> <li>• Deployed a long-term statistical simulation and modeling support plan for manufacturing.</li> <li>• Developed a statistical simulation training program for engineers and interns.</li> </ul>	
<b>System Engineer</b>	<b>2010-2011</b>
Thomas's responsibilities and accomplishments included the following:	
<ul style="list-style-type: none"> <li>• Developed and implemented a detailed product development procedure.</li> <li>• Focused on requirements capture and management for R&amp;D, operations, and IT.</li> </ul>	
<b>Education and Training</b>	
<b>Education:</b>	
<ul style="list-style-type: none"> <li>• M.B.A. in Management, Rockhurst University, Helzberg School of Management, MO, 2012</li> <li>• B.A. in History, University of Michigan, MI, 2004</li> </ul>	

### 7.4.2 Dan Ross (Identity Security Architect)

<b>Resource: Dan Ross</b>	
<b>Project Role:</b> Identity Security Architect	<b>Company:</b> Offeror employee 2012-Present
<b>Availability:</b> Starts on Contract Award	<b>Years of Experience:</b> 19
<b>Summary:</b>	
<p>Dan currently serves as Director of Clango's Privileged Access Management practice and as one of Clango's Senior Identity Security Architects. He has direct leadership and responsibility for delivery of identity security solutions, with a focus on the CyberArk PAM and Workforce Identity products. Apart from his leadership duties, Dan maintains an active role in client-facing project delivery as a Senior Identity Security Architect. This hands-on</p>	



**Resource: Dan Ross**

involvement keeps his technical skills current and deepens his insights into the practical challenges that Clango's customers face, enabling him to drive solutions that are both innovative and aligned with the latest industry developments. As an experienced software developer and cybersecurity engineer, Dan has a unique skillset well-suited to both the integration and customization of security solutions. He has worked with clients in various fields, including healthcare, education, finance, and government. He has a broad background in multiple disciplines of cybersecurity, including privileged access management, identity management and governance, access management, and fraud detection. His direct engagement in project work ensures that his leadership is informed by on-the-ground experience, making him an asset to both his team and clients.

**Systems Experience:**

- Programming: Java, JSON, XML, Eclipse, JDeveloper, SVN, Git
- Systems Design: Object-Oriented Design, Rapid Development, SDLC
- Security: Privileged Access Management, Identity Management, Risk Management
- Security Products: CyberArk, Oracle Middleware, Okta Workforce Identity

**Certifications:**

- CyberArk Guardian
- CyberArk Certified Delivery Engineer
- Certified Okta Developer
- Oracle Certified Associate, Java SE 7 Programmer
- ForgeRock Product Specialist

**Relevant Experience: Clango, Inc.****Director, Privileged Access Management****July 2021 - Present****Sr. Identity Security Architect**

As the Director of Privileged Access Management at Clango since July 2021, Dan is responsible for the delivery of comprehensive PAM and Identity Management solutions, primarily centered on CyberArk's suite, including Workforce Identity. His role encompasses crafting the strategic direction of the practice, ensuring that service offerings resonate with evolving market demands, and leading all aspects of his team's service delivery.

Key areas of responsibility:

- Overseeing the entire project lifecycle, from concept through to completion.
- Maintaining rigorous quality and client satisfaction standards.
- Leading the creation of best practices.
- Responsible for the advancement of the delivery team's expertise.
- Representing Clango in strategic client discussions and prominent industry forums.

**Identity Security Architect and Senior Developer****March 2012 - Present**

Dan has worked with various customers in the design, installation, development, integration, and administration of IAM and PAM solutions. His experience gives him insight into the challenges specific to both small and large organizations' use cases and solutions. Additionally, his development background and skills are advantageous in providing customization that may be required for different types of solutions. With his deep development skills, Dan has been involved not only in the development stage of the project but also the architecture and design of the solution.

**Resource: Dan Ross**

Dan's recent projects include working with:

- Financial Investment Company
- Fortune 50 Health Care Organization
- Department of Defense Customers

**Subject Matter Expertise:****CyberArk**

Dan has worked with various customers in the architecture, design, installation, integration, and administration of CyberArk PAM and Workforce Identity solutions. His experience gives him insight into the challenges specific to both small and large deployments in various fields. Additionally, his development background is advantageous in developing customizations such as custom PSM connectors and leveraging CyberArk's extensive API in DevOps operations. His responsibilities and accomplishments include the following:

- Reviewing organizational requirements and drivers to identify objectives, success criteria, priorities, CyberArk best practices, and use cases.
- Conducting an enterprise integrations review, including group policies, directory, authentication methods, monitoring strategies, and other relevant technologies and security tools.
- Reviewing systems requirements and prerequisites for deployment readiness, including change management and the change approval process.
- Providing guidance on break glass process design and procedures.
- Providing guidance to define roles and responsibilities, including those of core team members in deploying and managing CyberArk solutions.
- Installing, configuring, and hardening the CyberArk PAS Solution on DEV, Staging, Production, and DR servers hosting Windows Server OS including the following components: Vault, CPM, PVWA, PSM, and PSMP.
- Developing and customizing connectors and plug-ins based on customers' use cases.

**Okta**

Dan has extensive knowledge about how Okta enables User Lifecycle Management scenarios across cloud and on-premises solutions. He is familiar with the Okta Policy framework and how to control user access and map identity attributes and data transformations. Dan leverages both his lengthy history as a developer and his cybersecurity experience and certifications to build secure solutions using Okta APIs and SDKs. Dan uses his expert understanding of authentication and authorization standards such as OpenID Connect (OIDC) and OAuth and their support within Okta for building authentication, flexible authorization, and role-based access control. Dan also has experience configuring authorization with API Access Management and implementing Single Sign-On (SSO) with OIDC. His responsibilities and accomplishments include the following:

- Built custom OAuth 2.0 Authorization Servers to protect customer resource servers.
- Worked with customer to define and configure custom OAuth 2.0 scopes, claims, and access policies via the admin console.
- Prototyped API calls for distribution to applications owners.
- Prototyping possible solutions using OAuth and Microsoft Graph API.
- Integrating with Elasticsearch, Logstash, and Kibana (ELK stack) via the Okta API.

**Oracle**

Dan has extensive experience with Oracle Identity Suite and has developed custom integration around Oracle Fusion Middleware products and existing client web services for the purpose of improved security via identity

**Resource: Dan Ross**

management and strong authentication. He researched and designed solutions for development outside the scope of a straightforward installation and wrote custom access management rules used to flag risky behavior specific to the environment of each specific client. Dan also made use of the Oracle Fusion Middleware Java API to extend out-of-the-box functionality including native integration with one-time-password and flows for skipping security questions and retrieving a forgotten username. Dan's accomplishments and responsibilities include the following:

- Created training materials to be used by new employees unfamiliar with identity management.
- Leveraged the use of VMWare tools to develop in a distributed, virtual environment.
- Normalized existing data sources to be used for a universal risk management solution.
- Designed, implemented, and deployed access management plugins for a healthcare client.
- Developed and customized a fraud management solution for a client in higher education.

**Relevant Past Experience:****Pennsylvania Highlands Community College****Jan. 2014 - Present*****Mathematics Instructor***

Dan provides instruction and monitored teaching and learning effectiveness in various math courses including Business Math, Statistics, and Probability and Calculus.

**Indiana University of Pennsylvania (IUP)****Aug. 2011 - May 2012*****Mathematics Instructor***

Dan taught statistics and probability with material including descriptive statistics, sampling distributions, confidence intervals, and hypothesis testing. He managed two sections per semester and was responsible for all lesson plans, course materials, quizzes, and exams.

**Concurrent Technologies Corporation****Aug. 2004 – March 2012*****Software Engineer***

Dan worked on various Department of Defense (DoD) programs as a software engineer, systems engineer, and system integrator. He designed, implemented, and maintained the hardware and software baselines of multiple enterprise systems used at DoD installations worldwide. He conducted comprehensive code reviews aimed at improving the efficiency, readability, and robustness of the code. Dan also engineered software solutions that visually organized temporal and geospatial metadata from disparate sources, giving forward analysts the ability to quickly infer trends and relationships within time-sensitive data.

Dan's responsibilities and accomplishments included the following:

- Coordinated bi-weekly meetings to familiarize developers with emerging industry tools.
- Developed a fully functional XMPP chat client using the Java Swing API.
- Demonstrated company capabilities at various conferences and DoD locations.
- Helped design and construct a hardware solution consisting of multiple servers, SAN, LAN, and UPS capabilities.

**Education:**

**Resource: Dan Ross**

**Education:**

- MS, Applied Mathematics, Indiana University of Pennsylvania, 2010
- BS, Computer Engineering, The Pennsylvania State University, 2002

**7.4.3 Son Pham (Senior Identity Security Engineer)**

**Resource: Son Pham**

<b>Role:</b> Sr. Identity Security Engineer	<b>Company:</b> Offeror employee Nov. 2018-Present
<b>Availability:</b> Starts on Contract Award	<b>Years of Experience:</b> 32

**Summary:**

Son has over 30 years of IT industry experience, including cybersecurity engineering, team leading, and application development life cycle phases. He also uses his consulting, broad expertise in networking, system administration, compliance, support, troubleshooting, and efforts in the design/deployment space to assist clients on each project. Son is creative and an analytical self-starter with very effective communication and interpersonal skills, he has excellent problem-solving skills and a proven record of performance. His recent engagements include CyberArk development, implementation, and consulting for government agencies and regional utility companies.

**Systems Experience:**

- **COTS:** Siebel CRM (7.x, 8.x), AutoSys, SiteMinder 12.x
- **System Design:** Unix shell scripting, Perl, SQL, PL/SQL
- **Programming:** Java, C, XML, HTML
- **Databases:** Oracle, MS SQL server, Sybase
- **Operating Systems:** Windows Server, UNIX (Linux, Sun Solaris, AIX)
- **Security:** CyberArk (8.x, 9.x, 10.x, 11.x)

**Certifications:**

- CyberArk Certified Guardian (Level 4)
- CyberArk Certified Delivery Engineer (CCDE) (Level 3: Sentry)
- CyberArk Certified Privilege Cloud
- Siebel 8 Customer Certified
- AWS Certified

**Relevant Experience: Clango, Inc.**

**Cybersecurity Engineer** **Nov. 2018 – Present**

Son provides cybersecurity consulting services to meet the requirements of confidentiality, integrity, and availability for a range of government and commercial clients. He successfully completed multiple CyberArk implementation and consulting projects, including architecture design, software upgrade, and complex account onboarding. With his many years of experience in the IT industry, Son brings his knowledgeable skillset to help lead his team on CyberArk implementation for customers.

Son's responsibilities and accomplishments include the following:

**Resource: Son Pham**

- Managing and leading a team
- Consulting and working with customers on projects
- CyberArk implementation
- CyberArk Certified Guardian Level 4

Son's recent engagements include:

**CyberArk On-Prem projects: 2022-Present**

**Clango built out the client's On-Prem environments and migrated to their Production environment**

*Mattress Firm, Commercial Retail Southern Region Firm  
National Commercial Bank of Jamaica, National Financial institution  
Epson America, Commercial Printing Retailer*

**CyberArk Privileged Cloud projects: 2022-Present**

**Clango has built out the client's Privileged Cloud environments and migrated to their Production environment**

*Rutgers University, East cost University  
RiverStone, Midwest Construction Company*

**CyberArk Migration projects: 2022-Present**

**Clango has migrated the clients' existing PAM solutions to CyberArk Privileged Cloud**

*Red Wing Shoes, Midwest Retail Company  
Dexcom, West Coast Medical Device Company*

**Commodity Futures Trade Commission (CFTC), Government Agency – CyberArk Management Sept. 2020-2022**  
**Program Lead**

Son's responsibilities and accomplishments include the following:

- Assist the client with managing all account passwords
- Manage the client's current instance of CyberArk ICAM environment
- Advising the client on all aspects of CyberArk onboarding

**National Archives and Record Admin (NARA), Federal Government Agency – Onboarding CyberArk Oct. 2019-May 2021**  
**Technical Lead**

Son's responsibilities and accomplishments included the following:

- Onboarded new CyberArk environment
- Designed, implemented, and onboarded CyberArk for client
- Consulted the client on new environment

**San Diego Gas and Electric, Regional Utility Company – CyberArk Development Jan. 2019- Feb.2020**  
**CyberArk Engineer**

Son's responsibilities and accomplishments included the following:

- Developed customized plug-ins and tools for the client's CyberArk environment
- Communicated with the client to build and expand on their existing CyberArk application

**Relevant Past Experience: Fannie Mae**

**Senior Cybersecurity Engineer 2004 – 2018**

Son led a team to design and build a large-scale CyberArk implementation of Privileged Access Management to manage 20k+ account passwords on multiple platforms (Oracle, SQL server, Sybase, Active Directory, LDAP, UNIX), including most critical and sensitive financial applications.

### Resource: Son Pham

Son's responsibilities and accomplishments included the following:

- Managed multiple production and lower environments, including clustered vault, CPM, PWVA, PSM, PSMP, CCP and AIM providers.
- Worked extensively on a PSM connection component for multiple supported platforms and developing new plugins for non-supported platforms. Currently, he is working on onboarding UNIX root accounts.
- Served as the team lead for the CyberArk engineering team. He was involved in many aspects including monitoring, security compliance, performance tuning, architecture design, and scaling. He was responsible for planning and upgrading CyberArk software from v9.5 to v10.3 with minimal downtime. He worked closely with developers and CyberArk support to resolve issues and design new solutions.

#### **Senior Systems Engineer**

Son led a 24/7 support team that maintained high system availability for an Access Management system, providing authenticating and authorization for 250+ downstream applications.

Son's responsibilities and accomplishments included the following:

- Authoring and maintaining system designs and documentation
- Automating repetitive tasks
- System performance tuning
- System monitoring
- System architecture design
- In his role as a primary Siebel administrator, he designed, built, and maintained multiple environments of the Siebel 8.x Financials application, including Siebel Analytics, EAI, and Workflow. He was responsible for component monitoring, troubleshooting, system upgrade, deployment, user admin, and performance tuning.

### Relevant Past Experience: Oracle

#### **Principle Consultant**

**1999 - 2004**

Pham successfully implemented Siebel 7.5 Financial Services vertical application for a leading insurance claim company.

Son's responsibilities and accomplishments included the following:

- Designed a dynamic and real-time data validation engine
- Key member of a data integration team responsible for migrating and interfacing to legacy systems
- Designed and brought to production rollout a Siebel eCommunications implementation for a leading telecom company
- Worked as a primary technical architect and responsible for sizing, configuring, and maintaining all development, test, and production environments
- LDAP and Microsoft clustering admin, legacy data conversion, and database performance tuning.

### Relevant Past Experience: Technautics

#### **Oracle DBA and UNIX Systems Administrator**

**1997 - 1999**

Son worked as the primary Oracle DBA for multiple production databases, including the Injury and Unemployment Compensation database for the Dept. of Defense, the Bureau of Alcohol, Tobacco, and Firearms, and the Internal Revenue Service.

Son's responsibilities and accomplishments included the following:

- Coordinating database development and maintenance activities for database team members
- Managing user access
- Supporting client/server applications
- Performance monitoring and tuning
- Writing data loading scripts
- Automating application conversions
- Technical guidance for project managers

**Resource: Son Pham**

- Worked as a consultant for American Red Cross, Biomedical Information Services
- Responsible for configuring and maintaining 24/7 operation of a large-scale deployment of IBM RS/6000 servers
- Installed/upgraded system hardware and operating system
- Network troubleshooting
- Technical support to developers and end-users

**Relevant Past Experience: EDS**

**UNIX Systems Administrator** **1994 - 1997**

Son was responsible for DoD Civilian Personnel Management Service (CPMS) HP9000 servers and workstations. Son's responsibilities and accomplishments included the following:

- Managing daily operation of a technical team of HP-UX system admins and Oracle DBAs to support all critical production databases and software applications
- Installing/upgrading software
- Coordinating application development efforts
- Writing automation scripts for system monitoring
- Performance tuning
- Backup/recovery
- Providing end user tech support.

**Relevant Past Experience: IBM**

**Systems Engineer** **1991 – 1994**

Son was responsible for major functions including Detection, Track, and Localization in a real-time submarine AN/BQQ-5E sonar system.

Son's responsibilities and accomplishments included the following:

- Authoring Software Requirements Specification and test documents
- Designing, coding, testing and integrating the display subsystem
- Performing full cycle system test and certification
- Designing and simulating new functional capabilities in beamforming, track, and localization.

**Education and Training:**

**Education:**

- B.S. in Electrical Engineering, Computer Science, University of Utah, 1991

**Training:**

- AWS

## 7.5 Clango Services References

Clango has served hundreds of customers in the identity security space in all types of engagements, including advisory, installation, upgrades, migration, and operations & maintenance with CyberArk products. References from recent *Public Sector* services engagements are provided below. Additional references are available upon request.

### 7.5.1 State of Illinois

**Project Name: Identity Management Solution Advisory and Implementation Services**

<b>Client:</b>	State of Illinois Department of Innovation & Technology (DoIT)
<b>Contact Name:</b> <b>Contact Title:</b> <b>Contact Phone:</b> <b>Contact Email:</b>	Jennifer Rominger Security Program Manager <a href="mailto:jennifer.l.rominger@illinois.gov">jennifer.l.rominger@illinois.gov</a> 217-685-0819
<b>Project Overview/Summary:</b>	<p>The State of Illinois hired Clango to provide strategic IAM/IGA advisory and IAM implementation consulting services. During the initial phase of the project, Clango’s Identity Advisory team conducted discovery sessions with stakeholder groups to review and analyze the current state of the IAM program and processes and provide recommendations for improvements (programmatic and technical) <b>to manage identities across 63 different state agencies.</b></p> <p>Over the course of 18 discovery workshops with stakeholders, Clango performed assessments of current IAM/IGA processes, reviewed current documents and artifacts, and analyzed technology investments to identify the problems. We delivered a Comprehensive IAM Action Plan, a future-state IAM Reference Architecture, and an IAM Program Roadmap.</p> <p>Issues Identified:</p> <ul style="list-style-type: none"> <li>• 63 individual agency-specified IAM processes and tools, many with unique and disparate requirements.</li> <li>• Existing tools and processes not optimized for IAM best practices.</li> <li>• Proliferation of ambiguous use cases.</li> <li>• Lack of unified IAM vision resulting in low stakeholder consensus and ownership across state agencies.</li> <li>• No source of truth, incremental and incomplete transition from AD and other legacy sources to new statewide HCM system.</li> <li>• Critical need for an interim and immediate solution to gain traction and progress.</li> </ul> <p>Clango currently provides consulting, architecture, engineering, and management services to implement the following advisory recommendations our team delivered during the first phase of the project. The IAM solution our team is implementing is SailPoint’s IdentityNow SaaS solution.</p> <ul style="list-style-type: none"> <li>• Enact interim solution for aggregating sources of truth, providing authoritative sources to gain traction on critical goals (e.g., automations &amp; user certification) while minimizing agency impact and aligning with implementation of SuccessFactors.</li> <li>• Standardize on SuccessFactors, developing process improvements along with technology enhancements to streamline and standardize IAM processes across all agencies.</li> </ul>



	<ul style="list-style-type: none"> <li>• Develop and adopt an enterprise-level, global component, and process flow IAM architecture.</li> <li>• Utilize inventory of existing IAM tools per their relative strengths, best practices, and best fit to the State’s requirements.</li> <li>• Develop and adopt a cadenced communication process to foster participation and buy-in for accomplishing project goals as well as IAM program roadmap.</li> </ul>
--	---

### 7.5.2 State of Delaware

Project Name: CyberArk Implementation	
<b>Client:</b>	State of Delaware, Department of Technology and Information
<b>Contact Name:</b>	Navin Singhal
<b>Contact Title:</b>	Technical Project Manager
<b>Contact Phone:</b>	<a href="mailto:navin.singhal@delaware.gov">navin.singhal@delaware.gov</a>
<b>Contact Email:</b>	973-979-2500
<b>Project Overview/Summary:</b>	<p>Clango was hired to implement CyberArk’s Privilege Cloud solution (including CyberArk Identity) to establish a secure, streamlined, and scalable method of managing privileged credentials and reducing the attack surface that could be exploited by both external threats and insider risks.</p> <p>Clango completed an accelerated three-phase project that included discovery and planning, solution deployment, and operationalization. The following points summarize the activities and services delivered across the project stages:</p> <p><b>Discovery and Planning</b></p> <ul style="list-style-type: none"> <li>• Conducted a detailed PAM Program Workshop where Clango reviewed organizational requirements, success criteria, priorities, and timelines.</li> <li>• Conducted an analysis of critical risks and controls, utilizing Clango’s best-practice implementation recommendations to create a robust PAM roadmap.</li> <li>• Defined the roles and responsibilities of the State’s project team to ensure a seamless project flow.</li> </ul>

	<ul style="list-style-type: none"> <li>Facilitated an Architecture Workshop, resulting in a comprehensive architecture diagram that considered enterprise integrations, systems requirements, and change management processes.</li> <li>Gathered and document requirements via a series of facilitated meetings with the State’s project team.</li> </ul> <p><b>Deployment</b></p> <ul style="list-style-type: none"> <li>Executed a comprehensive deployment strategy that involved the installation, configuration, and hardening of various CyberArk PAM components, including Privilege Cloud Connectors, Session Managers, and Multi-Factor Authentication tenants.</li> <li>Validated the functionalities of the new Privilege Cloud environment and ensured successful integrations with LDAP, MFA, Remote Access, SIEM, and email notifications.</li> <li>Conducted rigorous testing of credential and session management for multiple platforms and facilitated Workforce Password Management integration.</li> <li>Demonstrated Offline Access functionality and established Dynamic Privileged Access for enhanced security.</li> <li>Provided comprehensive administrator training on the Privilege Cloud Solution to ensure efficient handover and future administration by State personnel.</li> </ul> <p><b>Operationalization</b></p> <ul style="list-style-type: none"> <li>Led Use Case Workshops to retrospectively review objectives and facilitate the onboarding of privileged credentials and integration of CyberArk solutions.</li> <li>Provided expert guidance on configuration and administration best practices and aided in the onboarding of additional remote access users.</li> <li>Shared insights into REST API functionalities, auditing, reporting, and monitoring capabilities of the PAM solution.</li> <li>Advised on the implementation of advanced and newly released features.</li> </ul>
--	--

### 7.5.3 Minnesota State University

Project Name: Identity and Access Management/Governance (IAM/IGA) Architecture and Engineering	
<b>Client:</b>	Minnesota State University
<b>Contact Name:</b>	Sam Buchannan
<b>Contact Title:</b>	Identity and Access Management

<b>Contact Email:</b>	sam.buchanan@minnstate.edu
<b>Project Overview/Summary:</b>	<p>Minn State University sought to replace the Oracle Identity Manager (OIM) with Microsoft Identity Manager (MIM). Clango provided Advisory services to build a target architecture and conversion plan. Clango provided Engineering services to actualize this plan. Minn State planned to join a single O365 tenant and move toward Azure AD, making it the central repository. Required functionality included synchronizing user identities from the system of record to enterprise AD. The final system functionality includes synchronization to three dozen universities in the Minn State University System.</p> <p>Clango performed the following tasks in support of this project:</p> <ul style="list-style-type: none"> <li>• Conducted onsite planning sessions to identify approach and methodology. Created project structure and implementation plan.</li> <li>• Conducted a structured requirements gathering process and development of prioritized requirements metrics.</li> <li>• Identified dependencies and risks that might affect the current environment, migration process, and production go-live in the new environment.</li> <li>• Developed an analysis document.</li> <li>• Created system, process, and technology designs.</li> <li>• Conducted a review of the current environment in preparation for new solution architecture.</li> <li>• Proposed a solution architecture and design for MIM implementation to meet the requirements of the new enterprise directory provisioning system at Minnesota State.</li> <li>• Clango’s engineering and integration resources deployed the solution in the testing environment in preparation for various security, regression, and performance tests to be performed.</li> <li>• Developed test plans, tested the MIM software, made necessary corrections, and conducted follow-up monitoring.</li> <li>• Collaboratively formulated a plan and set of activities to migrate existing data to production servers and performed the necessary data reconciliation activities.</li> <li>• Worked collaboratively with Minn State to develop rollout plans for campuses.</li> <li>• Developed On the Job (OJT) training for knowledge transfer, documented knowledge transfer content, and delivered training to system owners/administrators and end users.</li> <li>• Facilitated the handoff and transition to Minn State University Staff for ongoing operations.</li> </ul>

## 7.6 CyberArk Identity Solution References

CyberArk has over 8,000 customers across all industries and business sizes, over 800 of which have CyberArk Identity deployed. Any number of which would gladly offer themselves as references, including for example Spencer Stuart, American Bar Association, or the National Hockey League (US and Canada), which have successfully deployed CyberArk Identity in projects like that of the State of West Virginia.

CyberArk will be happy to facilitate an introduction between the State and some relevant customers as necessary.

Additional information and short case studies for the CyberArk Identity solution can be found below.



**PACIFIC DENTAL SERVICES**

### Defending Against Attacks & Driving Operational Efficiencies

Dental Support Organization Protects Staff and Dentists Across the U.S. With CyberArk

United States

**GOAL**  
Monitor and manage user access by protecting and controlling the large, dispersed growing number of privileged accounts, passwords, and mobile devices

**SOLUTION**  
Deploy CyberArk solutions comprising of three CyberArk applications: Privilege Cloud, Workforce Password Management, Endpoint Privilege Manager, and Secrets Manager

**RESULTS**

- Helps dentists increase productivity and spend more time on patient care
- Provides a clear and accurate picture of all privileged accounts
- Meets HIPPA standards for protecting patient healthcare information

“ For me, CyberArk is super important. If I take my security stack and look at the top three vendors we use, CyberArk is right up there. Knowing I can manage privileges and passwords and do so at scale without impacting the business is the biggest benefit I get from CyberArk.”

- Nemi George, CISO, Pacific Dental Services

Learn more at <https://www.cyberark.com/resources/customer-stories>



## Providing Secure Access And Protecting Data

Pharmaceutical Protects Its IP And Confidential Information Of Patients Participating In Clinical Trials

📍 Japan

### GOAL

Simplify IT processes and save money on managing multiple solutions to secure the access to business applications

### SOLUTION

Centrally manage user access to business resources across any device, anywhere, at any time combining SSO, MFA and VPN-less remote access

### RESULTS

- Secured remote access to internal web apps
- Integrated three separate tools and enabled cross communication
- Cost-effective solution
- Saved time and money for IT resources

“

*We had a quick meeting with CyberArk Professional Services where it created our account, talked us through the various settings and trained us to configure apps and policies.*

”

- David Howell, IT Associate Director at Chugai, Pharma Europe Ltd.

Learn more at: <https://www.cyberark.com/resources/customer-stories>

cyberark.com



## Enabling Efficiencies While Still Protecting Data

Electrical Utility Has Achieved A Secure, Cloud-Based Infrastructure

📍 Canada

### GOAL

Provide secure and frictionless access to cloud-based infrastructure

### SOLUTION

Centrally manage user access to business resources across any device, anywhere, at any time and streamline the management of application access requests

### RESULTS

- Achieved secure cloud-based infrastructure
- Reduction in service desk calls due to SSO
- Improved worker productivity
- Saved time and money

“

*CyberArk Identity helped us to become Ontario's first electrical utility to adopt a cloud-first infrastructure.*

”

- Mike Flegel, Cyber Security Specialist, London Hydro

Learn more at: <https://www.cyberark.com/resources/customer-stories>

cyberark.com





## Drives Flexibility Across The Business In Cloud-Based Infrastructure

Deliver Employees Single Sign-on Access To All Apps, Located In One Central Portal

 France

**GOAL**  
Support and secure the transform of the company into a more agile organization

**SOLUTION**  
Provide secure and frictionless access to business resources across any device, anywhere and streamline the management of application access requests

**RESULTS**

- Reduced help desk tickets and products to manage
- Productivity has improved
- Saved costs of a separate security solution
- Consolidated all identity management in one place

“

Security being paramount, we knew we'd need to transfer focus from the network and the devices to the applications: identity management would be essential to achieving these goals.

”

- Sébastien Huet, Chief Technology Officer, Remy Cointreau

Learn more at: <https://www.cyberark.com/resources/customer-stories> 



## Up-level Security

SBA Simplifies App Integration To Address MDM Requirements And SOX Compliance

 United States

**GOAL**  
Overcome high-cost disaster recovery as well as difficulties with implementation and management of the incumbent solution

**SOLUTION**  
Centrally manage user access to business resources across any device, anywhere, at any time combining SSO, MFA and VPN-less remote access

**RESULTS**

- Saved \$50,000 a year in AD FS costs
- Low maintenance requirements
- Strengthened security stature
- High Security

“

Now we count on CyberArk to effectively manage who we allow users into our environment.

”

- Jorge Grau, Senior Vice President and Chief Information Officer, SBA Communications.

Learn more at: <https://www.cyberark.com/resources/customer-stories> 



## Rapid User Onboarding And Off-boarding

Easy User Access To Critical Applications Whether Onsite Or Remote

United States

### GOAL

Provide secure and frictionless access to business resources across any device, anywhere, at any time

### SOLUTION

Adaptive authentication and single sign-on for cloud and on-premises applications and streamline the management of application access requests

### RESULTS

- Simplified device provisioning and management
- Increased security through two-factor authentication
- Easy user access to critical applications
- Saves time and money

“

*The beautiful thing about CyberArk Identity is that the user only has to remember one username and password -- all authentications happen behind the scenes.*

- Luis Mena, Director of IT, Early Learning Coalition ”

Learn more at: <https://www.cyberark.com/resources/customer-stories>

cyberark.com



## Strengthen Security And Reduce Complexity.

Enabling simple applications access for both remote and on-premise employees

Colombia

### GOAL

Increase security and reduce strain on the help desk – due to password reset requests – by providing employees with single sign-on (SSO)

### SOLUTION

Provide one-click secure access to cloud, mobile and legacy apps and streamline the management of application access requests

### RESULTS

- Increased visibility into outsourced IT activities
- End users are more productive and effective due to SSO
- Helpdesk calls have dramatically been reduced

“

*Rather than having to go through the usual process of contacting our services company, scheduling a meeting, gaining access to our servers and then ascertaining what had happened, we worked out the issue in real time*

-Paula Jaramillo, IT Coordinator, Grupo Argos ”

Learn more at: <https://www.cyberark.com/resources/customer-stories>

cyberark.com





## Implementing Cultural Change To Stronger Security

Avocado System Provides Access To Highly-Specialized Apps For The User

📍 New Zealand

**GOAL**  
Provide single Sign-on solution for Users engaged and using key apps

**SOLUTION**  
CyberArk Identity to easily provide and manage access across any device, anywhere, at just the right time

**RESULTS**

- Implemented widely accepted security practices
- Lower cost than building an in-house solution
- Stronger Security
- Able to track User Access

“

When I recommend a service provider to my clients, I want to be certain that once we're up and running, the client will be fully supported by the vendor. Our experience with CyberArk has assured me of that.

- Andrew Nimick, IT Consultant, NZ Avocado ”

Learn more at: <https://www.cyberark.com/resources/customer-stories>

cyberark.com



## Simplifying Password Management For Key Healthcare Apps

Simplified Authentication While Eliminating A Significant Percentage Of Help Desk Requests

📍 United States

**GOAL**  
Provide secure and frictionless access to business resources across any device, anywhere, at any time

**SOLUTION**  
Bring access management, provisioning and reporting together under one central solution to deliver greater simplicity, visibility and security

**RESULTS**

- Saving time and reducing costs
- Eliminating the percentage of help desk requests
- IT activities have been reduced
- Improved self-service user portal

“

With CyberArk Identity, we have a 100% cloud-based identity solution that provides authentication, provisioning and deprovisioning, MDM, Mac management, and the ability to track which users are logging into which apps and services.

- Steve Winter, IT Director at Apttus ”

Learn more at: <https://www.cyberark.com/resources/customer-stories>

cyberark.com





## Enable Operational Efficiencies & Satisfying Audit and Compliance

The Citizens Bank Gets Office 365 Federation and Meets GLBA Requirements with CyberArk

USA

### GOAL

Enable IT to focus more on strategic projects by simplify user provisioning and tighten access to customer data to meet GLBA regulation

### SOLUTION

Implementing CyberArk Workforce Identity helped federate access, set password management controls, MFA and single sign-on with one platform

### RESULTS

- Improved security compliance and assurance – raising NIST Cybersecurity Framework levels
- Helped meet strict cybersecurity and data protection regulations
- Increased staff productivity by simplifying daily operations and applications and data access

“

*I'd like to make it a policy that one of the criteria in accepting new vendors is that they integrate with CyberArk Identity to help us minimize risk, protect user data and remain within GLBA requirements.*

- **Ledale Reynolds**, CIO, The Citizens Bank of Philadelphia

”

Learn more at: <https://www.cyberark.com/resources/customer-stories>

cyberark.com 



556 B01 6 17:00 2373 04:05 A

556 B01 6 17:00 2373 04:05 A

Pcs: 1 1 of 1  
FID: 3964674 Rt#: 517  
INCORRECT ADDR  
04APR24 12:59  
Recpt Addr: 2019 WASHINGTON ST E  
Pkg Trk(s) #: 272919092373

Reused

TO REUSE: Mark through all previous shipping labels and barcodes.

ORIGIN ID: ZFOA (000) 000-0000 SHIP DATE: 02APR24  
STEVEN GRUSZ ACTWGT: 0.40 LB  
2107 HILSON BLVD CAD: 6991667/SSFO2500  
SUITE 250  
ARLINGTON, VA 22201 BILL CREDIT CARD  
UNITED STATES US

TO DEPT. OF ADMIN PURCHASING DIV.  
ATTN: LARRY D. McDONNELL, BUYER  
2019 WASHINGTON STREET EAST  
CHARLESTON WV 25305  
(304) 668-2083 REF: DEPT:  
FedEx Express

TRK# 2729 1909 2373 WED - 03 APR 5:00P  
STANDARD OVERNIGHT  
XS CRWA 25305  
WV-US HTS  
Barcode

VENDOR NAME: CLANGO, INC  
BUYER: LARRY D. McDONNELL  
SOLICITATION NO: CRFP 0947 ERP2400000002  
BID OPENING DATE: APRIL 4, 2024  
BID OPENING TIME: 1:30 PM EST.  
FAX NUMBER: 304-558-3970