IDENTITY AND ACCESS MANAGEMENT (IAM)
MANAGED SERVICE SPECIFICATION

Prepared for:
GCloud 15

Disclaimer
ProofID Limited makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

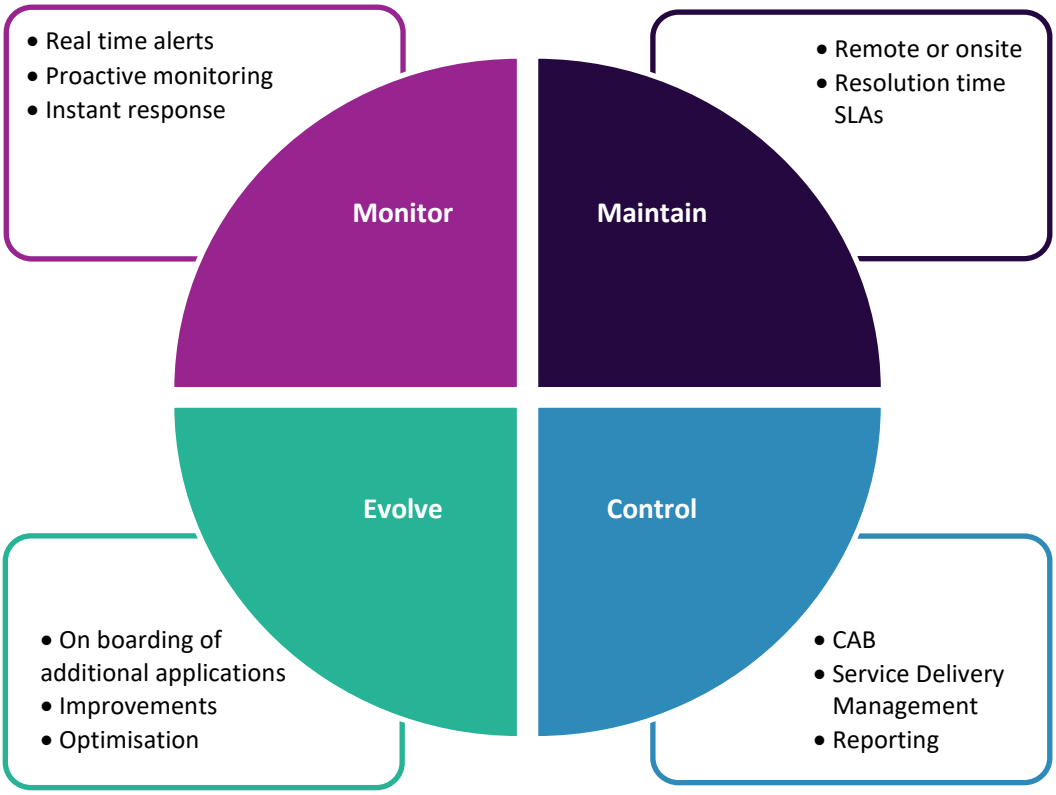
Contact
Questions related to the information contained in this document should be directed to ProofID Sales at sales@ProofID.com
Tel: +44 (0)330 808 0785

ProofID Ltd
Building 8
Exchange Quay
Salford, M5 3EJ

1. IAM MANAGED SERVICE INTRODUCTION

This section provides a general overview of the IAM Managed Service provided by ProofID and is for informational purposes only. The specific deliverables of the Customer's IAM Managed Service are described in section 2, IAM Managed Service Design.

The illustration below summarises the four components of the IAM Managed Service.



1.1 Monitor

ProofID can continually monitor the Customers application environment via a site to site VPN connection.

Any outages or unusual conditions will raise an alert which will be reported in real time at the ProofID's offices. Additionally, alerting emails and SMS text messages will be sent to the IAM Managed Service team, and a new incident will be automatically opened in the ProofID's call tracking system.

Upon receipt of an alert, work will begin immediately to identify and remedy the issue.
ProofID aims to resolve the issue before it has become a problem for end users, and always within the agreed resolution time SLAs.

ProofID will also analyse remote monitoring data over time to produce benchmarking statistics, and to identify and address reoccurring or underlying conditions.

1.2 Maintain

ProofID can assume full responsibility for all maintenance activities relating to the identity management environment.

Maintenance includes all Business As Usual (BAU) activities such as:

- Security Patches.
- Software Updates – Minor Versions
- Operating System Health checks of the application

Security Patch Definition

A security patch is a piece of software released by a vendor via a Security Advisory notice which corrects a security vulnerability identified by the vendor.

Minor Version Definition

As ProofID cannot control the contents of releases from software vendors, Minor Version is defined as a software release which meets the following characteristics:

- Released as an increment to the minor version number e.g. 4.1 to 4.2.
- Can be deployed as a single software package to each affected server.
- Does not require changes to existing configuration in order to maintain current deployed functionality.

Each potential release will be assessed for compatibility with the above definition via examination of the release notes and/or discussion with the vendor.

Releases which do not meet this definition will be classed as Major Versions; as such their deployment will consume Evolve Hours.

All maintenance activities will be carried out in pre-production and production environments to ensure that both environments remain synchronised.

The ProofID will resolve all technical support incidents, whether raised automatically though the remote monitoring service, or raised as required by Customer Support Representatives (CSRs). Support resolution is fully active, meaning that the Supplier Support Representative (SSRs) will connect remotely to the customer site via the VPN and will work on the issue until it is resolved.

ProofID can maintain relationships with system owners and administrators for all systems which fall within scope of the identity management system. This is important in ensuring prompt resolution of support issues. By way of example, if there is a problem relation to data held within the HR system which prevents synchronisation of user data through the identity management system, The SSR will contact the HR system administrator directly and will work with them to identify and rectify the issue.

Business As Usual (BAU)

- Incident logging
- Troubleshooting Incidents where the issue is with the solution ProofID manages.
- System patching of the application (Bug fixes and security patches)
- System updated of the application (deployment of minor version updates)
- Certificate updates for the application
- Out of Hours activity; Priority 1 and 2 only where the issue is with the solution ProofID provide.
- Tasks Where Service Hours Are Consumed

BAU does not include:

Service Hours incidents that occur where the issue is not with the solution ProofID provides. E.g. changes made client side.

- Delivery of Change Requests to the configuration as a result of an Incident investigation where the solution was working as designed.
- Delivery of Service Requests. E.g., modify/adding new functionality to the current configuration.
- Changes which are a result of troubleshooting an incident where the solution is operating as designed.
- System upgrades (deployment of major version upgrades) – Major version meets all software updates which do not meet the definition of Minor Version or Security Patch in section 1.2 above.
- Out of Hours activity, Priority 1 and 2 incidents where the issue is not with the solution ProofID manages (charged at double rate).

The service hours can additionally be used for project work, to add new functionality and amend existing functionality.

1.3 Control

ProofID will participate in the customer's change control procedures where required to ensure that all changes to the identity management environment are subject to good governance and tried and tested processes. This is imperative to ensure that there is no unexpected downtime affecting the identity management environment and its connected systems.

All changes to the identity management environment will be tested and deployed in the pre-production environment (where one exists) first before deployment to production. Any lessons learned from the pre-production deployment will be taken into account during the eventual production deployment, minimising any risk of outage.

ProofID will assign a Service Delivery Manager (SDM) who will be responsible for the quality of the work delivered under the IAM Managed Service. The SDM will produce monthly reports detailing performance of the contract and will arrange for monthly service review meeting or conference calls with an option of an Onsite quarterly meeting.

1.4 Evolve

A key focus of the ProofID IAM Managed Service is continual evolution of the identity management environment.

Evolve Hours can be used to deliver non-BAU requirements, such as development and implementation of a new identity management connector or protected application, or implementation of previously unused functionality, which is available in the licensed identity management product.

ProofID will work with the customer to identify potential service improvements in line with the Customer's business drive and will plan and execute their implementation by means of the Evolve Hours.

ProofID will discuss priorities for this during monthly IAM Managed Service review meetings.

2. IAM MANAGED SERVICE DESIGN

This section describes the specific service that will be provided by ProofID to the Customer.

The following may also be included as part of the Managed Services:

- Strategic IAM roadmap, Cloud Migration Planning and setup and migration services across platforms or developing and implementation of new a new system
- Quality and Assurance performance testing of the IAM system
- Provide complete training on IAM/IGA platforms (configuration, administration and end user training)

2.1 Agreement Period and Timeline

To be agreed.

2.2 Items in Scope for the IAM Managed Service

The components which comprise the services covered by the IAM Managed Services will be defined in the Service Catalogue that is held in the Customer's area on ProofID's secure intranet. The Service Catalogue will be prepared as part of the Onboarding Service. .

The Service Catalogue will have been agreed prior to commencement of the service. Thereafter the Service Catalogue from time to time will be subject to continuous review via the monthly review meetings and will be updated quarterly (by ProofID) as agreed at the monthly review meetings. One month after any such update the parties will be deemed to have approved the adoption of any such quarterly update to which they have not objected, and in particular this shall serve as notice to the

Customer to check the IAM Managed Service specification quarterly, within a month of the quarter-end, for changes to that specification.
Any changes or additions to the service catalogue will incur additional IAM Managed Service fees.

In summary, the scope of the IAM Managed Service will include the following components:

Application	Supported hours	Operational Management	Implement change?	Troubleshoot / debug?
		Yes	Yes	Yes

2.3 Items outside Scope for the IAM Managed Service

Service boundaries define the limits of the scope of the IAM Managed Service. ProofID's responsibilities extend as far as the service boundary; maintenance of elements beyond the service boundary is the responsibility of the Customer or its agents. Items inside the service boundary will be specified in the Service Catalogue.

The service boundaries are typically agreed and documented during the Onboarding Service, but as a rule of thumb, ProofID will maintain all elements of the identity management environment, up to the point of integration with target or source systems, which is typically a software agent running on the connected system server.

2.4 IAM Managed Service Deliverables

DELIVERABLE	DESCRIPTION
MONITOR	
Will monitoring be provided?	YES
Monitoring Scope	TBA
VPN Scope	
MAINTAIN	
Business as Usual (BAU) activities	• Incident logging • Troubleshooting Incidents where the issue is with the solution ProofID manages. • System patching of the application (Bug fixes and security patches) • System updated of the application (deployment of minor version updates) • Certificate updates for the application • Out of Hours activity; Priority 1 and 2 only where the issue is with the solution ProofID provide.
Technical Support	During Normal Business Hours, ProofID will provide third line support for the components described in 2.2 and in more detail in the Service Catalogue which will be completed on completion of the Onboarding

	Service. ProofID will assume responsibility for resolution of incidents and will liaise with the Customer, and Customer's Suppliers as required to resolve the incident, acting at all times within Customer's prevailing change control procedures. Outside of Normal Business Hours, ProofID will provide support for the system on P1 Incidents. P1 incidents logged out of hours, which are outside of ProofIDs service boundary shall be charged from Service Hours at double time.
Access to Technical Support	Should the Customer determine that the IAM Managed Services includes a defect, the CSRs in Schedule 4 may file error reports, or support requests. ProofID shall provide technical support services only to the specified CSRs in Schedule 4.
Root Cause Analysis (RCA)	Root Cause Analysis (RCA) will be produced within 5 working days of resolution for Priority 1 incidents.
Environments in scope	Refer to: 2.2 Items in Scope for the IAM Managed Service
Method of Access	VPN – Subject to method of access to be agreed in discovery phase.
Incident management	ProofID shall accept E-mail and web form-based incidents submitted from CSRs 24 hours a day, seven days a week, 365 days per year. All Priority 1 incidents should be submitted by Telephone. ProofID shall accept telephone calls in English language during Normal Business Hours. The ProofID shall process support requests, issue trouble ticket tracking numbers if necessary, determine the source of the problem and respond to the Customer in accordance with section 2.5. If no progress has been made on a Priority 1 or Priority 2 incident within the target resolution time as set out in section 2.5., The incident shall be escalated to the SDM. If the incident is not resolved, then after each successive increment of the target resolution time the incident shall be escalated to the ProofID Manager of IAM Managed Services, Followed by SVP of Delivery, followed by the EMEA CEO. The Customer shall provide front-line support to other IAM Managed Services users who are not the designated CSRs. However, the Customer's designated CSRs may contact ProofID IAM Managed Service in order to report problems that the Customer's designated

	CSRs cannot resolve themselves after they have performed an initial level of diagnosis. The detailed process for Incident management will be agreed as part of the Onboarding Service.
CONTROL	
Service Delivery Manager (SDM)	A Service Delivery Manager will be allocated to the Customer by ProofID to assume overall responsibility for delivery and quality of the IAM Managed Services
Service Review Meetings	Monthly service review meetings to review incidents and activities during the previous month, and performance against Service Level Agreement (SLAs). These meetings may take place onsite at the Customer's offices, at ProofID's offices or via conference call or web-meeting technology, as agreed by the parties. The parties shall agree the schedule for the monthly service review and Improvement Workshop within the first month following the Contract Start Date. The meeting will be documented by the Service Delivery Manager and actions circulated after the meeting.
Quarterly IAM Managed Service Review Meetings	Quarterly IAM Managed Services review meetings will be held to review the overall performance of the IAM Managed Services. These meetings will take place onsite at the Customer's offices, at ProofID's offices or via conference call or web-meeting technology, as agreed by the parties
Reports	The following regular reports will be provided: **Monthly IAM Managed Services Report** – This report will be produced monthly one week prior to Service Review meeting, and covers: • Breakdown of incidents handled • Breakdown of problems handled • Major issue Root Cause Analysis summary and actions • Summary of maintenance performed during the period • Summary of planned maintenance for the next period • Proposed service improvements • Service Hours usage summary **SLA Review**

	Evolve Hours Usage Report – This report will be produced monthly one week prior to the service meeting and will contain: • Detailed breakdown of Evolve Hours used to date, including detailed reasons for usage **Root Cause Analysis –** to be produced following any major (P1 or P2) incidents. The report will contain: • Description of major incident • Incident resolution • Detailed information as to why the incident occurred • Action plan to prevent/mitigate against recurrence
CAB Attendance	Participation including attendance via conference call at Change Advisory Board (CAB) meetings. The IAM Managed Service limits the attendance at CAB to 26 per annum. CAB attendance after 26 will be chargeable through Evolve Hours.
Change Control Documentation	Preparation of Change Control documentation as per the change control process for all changes.
Test	All changes will follow the Change Control Procedure
EVOLVE	
Improvement Workshop	One annual Improvement workshop, to take place within the first six months of the contract year, to identify potential system improvements in line with the customer's business drivers.
Evolve	The number of Evolve Bank Hours provided is specified in Schedule 1 – IAM Managed Service Fees. Evolve Hours charged in the following way: • Onsite work is chargeable in 8 hour blocks. • Remote work is chargeable in 1 hour blocks. • On a Time & Materials basis. • Where consultancy work which has been agreed, scheduled, and cancelled at short notice, the Customer will be charged at the rate

	already agreed (Daily rate/OHH). The Customer must give notice of any cancellations; • Two working days' notice is required by the Customer for cancellations of planned work of five working days or less. • Five working days' notice is required by the Customer for cancellations of planned work of 6 working days or more. • The client must cover any travel cost incurred during any cancellations notwithstanding of giving notice. • Out Of Hours (OOH) work is charged at double rate.

Support Hours

- Normal support is provided during Core Business Hours (09:00 – 17:00 GMT Monday to Friday)
- Out of hours' support is provided outside Core Business Hours (17:00 – 09:00 GMT and Saturday/Sunday)

2.5 Service Level Agreement

Priority	Response Time	Resolution Time
P1 Incident	30 Minutes	4 Hours
P2 Incident	30 Minutes	8 Hours
P3 Incident	1 Hour	16 Hours
P4 Incident	4 Hours	4 Days
Service Request	1 Day	10 Days

Supported Technologies

ProofID is vendor agnostic and supports a wide array of identity management products, including:

- Ping Identity PingFederate, PingAccess, PingOne, PingDirectory, Ping Intelligence and PingID
- SailPoint – All products, modules and connectors
- NetIQ IDM and Access Manager
- Delinea PAM product suite
- CyberArk – All products, modules and connectors
- Shibboleth
- Microsoft
- ProofID products

Licencing can be provided as part of the Managed Services for SailPoint, Ping Identity and CyberArk products subject to agreement.