



Principle
Networks

Service Description - Okta Managed Service

Table of Contents

Introduction	4
Okta Managed Service Overview	5
About Okta	6
Okta Managed Service	7
Specialist Okta Support	7
Okta Platform Operations and Monitoring	8
Universal Directory	8
Single Sign-On and Application Integrations	9
Multi-Factor Authentication	9
Lifecycle Management	10
Workflows	11
Identity Governance	12
Device Assurance and Context	12
Okta Device Access	12
Identity Threat Protection	13
Identity Security Posture Management	13
Privileged Access	14
Access Gateway	14
Secure Partner Access	14
Auth0	15
Service Optimisation	16
Configuration Hygiene	16
Continuous Enhancements	17
Regular Business Reviews	18
Service Management	19
Incident Management	21
Request Management	21
Change Management	21
Problem Management	23
Proactive Monitoring	23
Low-Priority Issues	23
Continuous Service Improvement (CSI)	24
Change Hours Contracts	25
Ad-Hoc Service Reporting	26

Principle Networks Customer Portal	26
24x7 Service Operation	26
Access to 3rd line engineers	26
Co-Management Arrangements.....	27
Escalation and Management	27
Service Levels (SLAs).....	28
Escalations Process.....	29
Complaints Process	29
Document Control, Detail and Change	30

Introduction

This document describes the **Okta Managed Service**, service levels and enhanced options provided by Principle Networks. This Service Description applies specifically to Principle Networks' Okta Managed Service.

This Service Description is provided as a supplement to Principle Networks General Terms and Conditions. Principle Networks may update this Service Description from time to time without notification.

Our solutions, services and support are certified against the following standards:



Principle Networks are an Authorised Okta Partner and Okta Managed Service (MSP) Partner.

Okta Managed Service Overview

Principle Networks offer the following list of services as part of the managed service. Enhanced options are available to add-on to the managed service during the sales process and in-line with ordered Okta licensing, not included as part of the managed service.

Please note that Enhanced options will be defined within the Scope of works. These options can be combined or can be selected on their own.

Service Description	Managed Service	Enhanced Options
Specialist Okta Support	✓	
Okta Platform Operations and Monitoring	✓	
Universal Directory	✓	
Single Sign-On and Application Integrations	✓	
Multi-Factor Authentication	✓	
Lifecycle Management	✓	
Workflows	✓	
Identity Governance		✓
Device Assurance and Context		✓
Okta Device Access		✓
Identity Threat Protection		✓
Identity Security Posture Management		✓
Privileged Access Management		✓
Access Gateway		✓
Secure Partner Access		✓
Auth0		✓
Service Optimisation	✓	
Configuration Hygiene	✓	
Continuous Enhancement	✓	
Regular Business Review	✓	
Service Management	✓	
Change Hours Contracts		✓
Ad-Hoc Service Reporting	✓	
Principle Networks Customer Portal Access	✓	
24/7 Servicedesk	✓	
Access to 3 rd Line Engineers	✓	
Co-Management Arrangements	✓	
Escalation Management	✓	

Details of the services offered above can be found throughout this document.

About Okta

Okta is a cloud-based identity platform that provides a central control point for authentication, access, identity lifecycle and identity-driven automation across an organisation. Okta securely connects modern cloud applications, legacy directories, on-premises systems, infrastructure and multiple

existing identity sources into a consistent identity architecture. This allows organisations to move away from less secure fragmented identity silos and manage access through a common set of policies, processes and security controls regardless of the application or identity source.



Organisations are adopting Okta because identity environments have become increasingly complex. Users may exist across legacy LDAP directories, Active Directory domains, cloud directories, acquired business units and application-specific identity stores, each with different authentication methods and administrative overhead. Okta helps bring these environments together without requiring every underlying platform to be replaced, providing a consistent identity layer umbrella across the whole organisation. This capability is particularly valuable following mergers and acquisitions, where different business units may need to retain existing systems and identity providers while still operating within a unified access and security model.

Okta extends industry leading secure authentication beyond traditional SaaS applications. By utilising Okta, organisations can apply modern authentication and phishing resistant MFA requirements to applications, administrative access and server or infrastructure that previously have relied on passwords or locally managed credentials. Centralised policy and contextual access controls improve security while reducing friction and the need to manage separate authentication mechanisms across different technology platforms.

Beyond authentication, Okta significantly reduces the administrative burden associated with managing user identities. Joiner, Mover and Leaver processes are often dependent on service desk tickets, manual account creation, group changes and individual application administrators, creating delays and opportunities for human error which result in exploitable vulnerabilities within an organisations. Okta orchestrates these processes using lifecycle management and workflow automation, automatically creating, modifying and removing access as users join, change job roles or leave the organisation altogether. The result is a more consistent and auditable identity lifecycle, faster access for users, reduced operational effort for IT teams all while removing human error and closing the loop on the possibly of security exposure.

Okta Managed Service

Principle Networks provide ongoing operational management, support and optimisation of our customer's Okta environments. The service is designed to maintain a secure, reliable and manageable identity platform while ensuring that the environment is continually enhanced to support changing organisational needs, applications and security requirements.

The service extends beyond the initial configuration of Okta and the onboarding of new integrations. Principle Networks provide day-to-day technical support, respond to relevant Okta alerts and platform issues, undertake regular operational checks and maintain oversight of the configuration and health of the solution.

Where issues occur, Principle Network's servicedesk investigate the underlying Okta configuration and take appropriate corrective action within the defined Service Level Agreement. Recurring issues, configuration weaknesses, technical debt and opportunities for improvement will be regularly reviewed as part of the ongoing management of the platform.

The precise scope of Principle Networks managed service must reflect the Okta products and subscriptions licenses ordered by each customer.



Specialist Okta Support

We understand Okta's solution offering intimately and have a proven record of accomplishment with customers for delivering excellent solutions within Okta's platform, delivering confidence that your environment is well managed and secure. Like all areas of Principle Networks' service, we provide access to our experienced 3rd line Certified support engineers to get problems and queries resolved quickly. Our goal is to minimise prolonged email exchanges that do not lead to resolutions. We encourage our engineers to proactively engage with customers via phone conversations to fully discuss and comprehend the issues at hand.

Principle Networks, as necessary add policies and controls to the customer Okta tenant. With customer approval, our engineers can produce detailed Change Requests that are reviewed and approved internally before being sent to you for your own internal review and approval. We then implement these Changes within your Okta environment at a window agreed by you and monitor the completed change against success criteria.

Okta Platform Operations and Monitoring

Principle Networks provide operational oversight of your Okta tenant and use available platform information including the Okta System Log, reports, Health Insight and relevant security events to identify conditions requiring investigation.

Where appropriate, Principle Networks define and implement monitoring and alerting for events that require operational intervention, proactively raising possible problems to our servicedesk for investigation and to resolve identified issues. This may include suspicious administrative changes, authentication issues, integration failures, security events and other conditions relevant to your specific Okta environment.

Principle Networks will investigate detected issues and determine whether they originate from the Okta service, tenant configuration, identity source, application integration or another dependent system. Where required, Principle Networks coordinate with Okta Support directly or other relevant 3rd party parties while retaining ownership of the issue through the managed service.

Universal Directory

Okta Universal Directory provides a central identity store for users, groups, devices and identity attributes and allows identity information from HR platforms, Active Directory, LDAP and other sources to be represented consistently within Okta.

Principle Networks manage the Universal Directory configuration within the agreed scope of each customer's Managed Service. Changes to identity sources or organisational structures can cause mappings, attributes and group logic to become unnecessarily complex over time. We maintain ongoing oversight of these dependencies and investigate and resolve issues such as incorrect attribute values, unexpected profile updates, duplicate identities or unsuccessful directory synchronisation.

As your organisation changes, Principle Networks ensure that Universal Directory continues to provide a clear and supportable identity model upon which authentication, provisioning and governance policies can be depended on reliably.

Single Sign-On and Application Integrations

Okta Single Sign-On (SSO) provides users with centralised access to applications using federation technologies including SAML, OpenID Connect and native Okta connectors, reducing reliance on separate application credentials, allowing access controls to be applied consistently through Okta. Some of these integrations enable user accounts and attributes to be created, updated and deactivated automatically in downstream applications.

Principle Networks support and manage existing SSO integrations, create new ones and assist with changes required as applications, certificates, endpoints or authentication requirements change. We work with your application providers to support updates and changes to SSO integrations. Principle Networks maintain awareness of upcoming certificate expirations and other integration dependencies, eliminating avoidable service disruption.

Repeated application sign-in failures are investigated using relevant Okta events and application configuration, including federation settings, claims, attribute mappings, certificates and application-side dependencies.

Principle Networks will also identify applications where authentication has been integrated with Okta but lifecycle management remains manual. Where appropriate, opportunities to introduce provisioning or improve the application's access model will be discussed as part of our Regular Business Review process, described later in this document.

Multi-Factor Authentication

Okta MFA and Adaptive MFA strengthen authentication by requiring additional assurance based on factors such as the authenticator being used, user context, device context and applicable sign-on policy. Okta FastPass provides phishing-resistant, passwordless authentication through Okta Verify and can reduce dependence on passwords and traditional push-based MFA.

Principle Networks will manage the customer's configured Authentication policies, Authenticator Enrolment Policies, Global Session Policies and App Sign-In Policies within the agreed scope.

Authentication incidents will be investigated to establish whether access has been affected by new policies, user enrolment, device state, authenticator behaviour or another dependency.

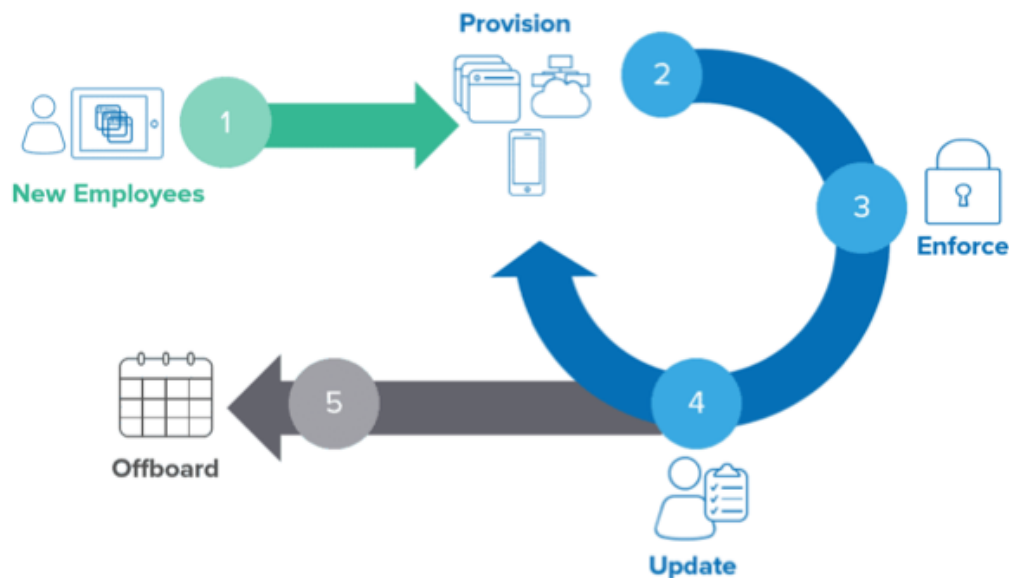
Principle Networks will periodically assess the authentication configuration for unnecessary exceptions, overlapping rules and legacy authentication methods. Where appropriate, recommendations will be made to increase the adoption of stronger authentication methods such as Okta FastPass and FIDO2 WebAuthn while maintaining an appropriate user experience.

Our objective is to maintain authentication controls that remain secure without becoming unnecessarily complicated as additional applications, user populations and access requirements are introduced.

Note that customers must hold the Adaptive MFA licensing to utilise Adaptive MFA within their tenant.

Lifecycle Management

Okta Lifecycle Management automates the creation, update and removal of access as users join, move within or leave an organisation. It can use authoritative identity sources, group membership, application assignments and provisioning integrations to reduce manual administration and ensure changes are consistently reflected across connected applications.



Principle Networks support and manage the lifecycle configuration within your organisation, including provisioning integrations, application assignments, Group Rules, Profile Mappings and associated joiner, mover and leaver processes. Provisioning failures affecting individual users are investigated and resolved through normal operational support. Principle Networks will also monitor for recurring failures or patterns that indicate a wider problem with an application connector, SCIM integration, attribute mapping or lifecycle process.

As the organisation changes, Principle Networks will assess whether existing lifecycle rules continue to reflect the customer's structure and access model. Particular attention is given to mover processes and exceptions where users could otherwise accumulate access as their role changes.

Our objective is to maintain lifecycle automation as an effective business process rather than allowing it to gradually become dependent on manual workarounds and exceptions, reducing administrative burden and saving your teams time to spend on more valuable activities.

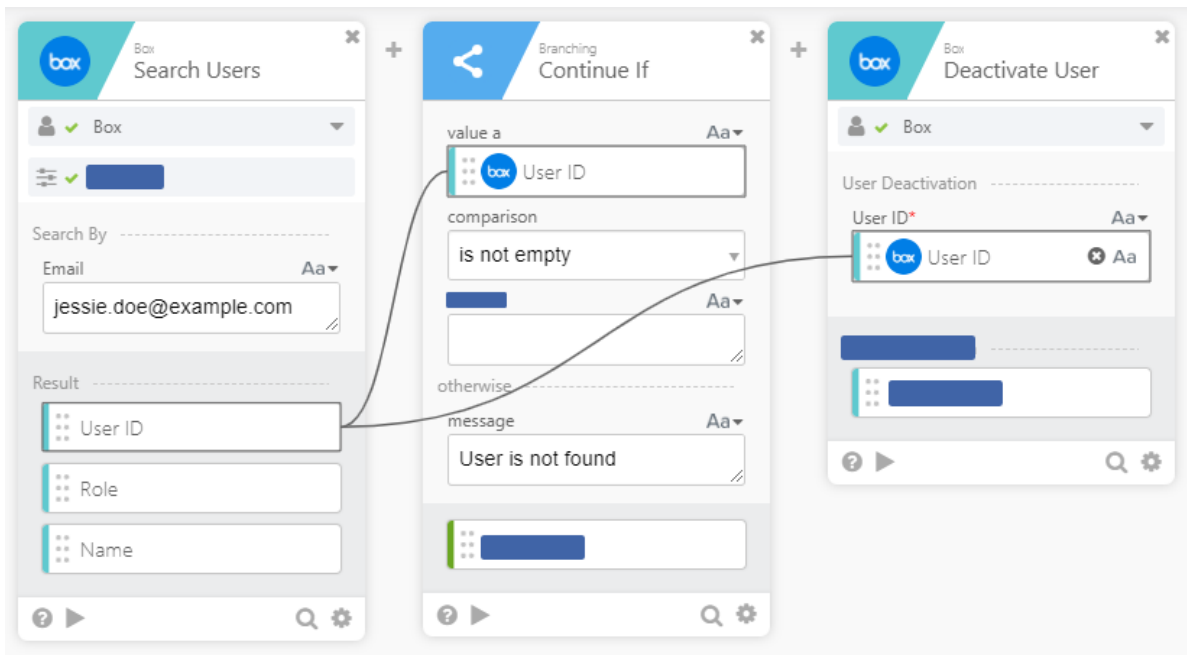
Workflows

Okta Workflows provide a no-code automation and orchestration platform for identity-related processes. They can extend the standard capabilities of Lifecycle Management and other Okta products by automating multi-stage processes, interacting with third-party applications and APIs, generating notifications and responding automatically to identity or security events.

This allows organisations to remove repetitive manual tasks and replace bespoke scripts with controlled identity automation.

Principle Networks will support and maintain Okta Workflows included within the customer's managed service scope. This will include investigation of failed flows, connector or connection issues, unexpected workflow behaviour and changes to dependent systems that affect existing automation.

Principle Networks will maintain awareness of the purpose and dependencies of managed flows so that changes can be implemented safely. Where organisational processes change, existing workflows can be amended to reflect new joiner, mover, leaver, approval or operational requirements.



Principle Networks will also identify opportunities where recurring manual identity administration could appropriately be replaced or improved using Okta Workflows.

The objective for our managed service is, through Workflow automation to evolve with the customer's organisation rather than becoming a collection of undocumented processes that are difficult to safely modify.

Identity Governance

Okta Identity Governance extends identity lifecycle management by introducing formal controls around requesting, approving, reviewing and removing access. Capabilities include Access Requests, Access Certifications and Entitlement Management, allowing organisations to demonstrate not only that a user has access but why it was granted and whether it remains appropriate.

Principle Networks support the operation of configured governance processes and assist with the management of Access Requests, approval processes, resource ownership, entitlement structures and Access Certification campaigns.

Where campaigns or access requests generate exceptions or operational issues, Principle Networks' servicedesk investigate configuration and workflow dependencies as appropriate.

Principle Networks will help your teams develop the coverage of Identity Governance over time. This may include introducing additional applications or entitlements into governance, improving reviewer context, reducing permanent access and identifying areas where repeated certification decisions indicate that the underlying access model should be improved.

Our objective is to move the organisation towards demonstrable least-privilege access without introducing unnecessarily friction through burdensome governance processes.

Device Assurance and Context

Okta Device Assurance allows device security characteristics to be incorporated into access decisions. When combined with Okta Verify, FastPass and App Sign-In Policies, this allows access to applications to consider both the identity of the user, the context of their access and the security posture of the device.

Principle Networks support configured Device Assurance Policies and investigate access issues where device posture contributes to an authentication decision. As endpoint standards change, Principle Networks will work with you to ensure that Okta Device Assurance requirements remain aligned with the relevant device management and security controls. This provides customers with the ability to strengthen access decisions beyond username and MFA alone while avoiding policy requirements that no longer reflect the organisation's managed-device standards.

Okta Device Access

Okta Device Access extends identity controls to the device sign-in experience and includes capabilities such as Desktop MFA and Desktop Password Sync. This enables organisations to apply Okta-based identity assurance at device login as well as when users subsequently access applications.

Where Okta Device Access is included within the managed service, Principle Networks support its configuration and operation and investigate issues affecting device enrolment, Desktop MFA, authentication or associated policy behaviour. Principle Networks work within your organisation's endpoint management processes where configuration dependencies exist and help maintain alignment between Okta authentication requirements and the managed device estate.

Identity Threat Protection

Identity Threat Protection continuously evaluates identity, device and session context after the initial authentication event and can trigger responses when user risk changes. Responses can include step-up authentication (ODIC only), session termination and Universal Logout across supported applications.

Principle Networks support the configuration and operation of Identity Threat Protection policies and associated integrations within the agreed service scope. Relevant identity threat events may be integrated into your internal monitoring platforms and incident processes so that events requiring investigation can be acted upon promptly. Typically these are forwarded to an inhouse SIEM or 3rd party MDR platform.

Principle Networks will periodically assess the effectiveness of configured responses and identify opportunities to improve integration between Okta and other security technologies providing risk signals.

Please note that while Principle Networks will always support our customer's with high risk events to investigate and remediate critical security issues within their Okta environment. Our Managed Service does not however profess or offer or replace a dedicated SOC or an MDR service.

Identity Security Posture Management

Okta Identity Security Posture Management provides continuous visibility of identity risks across Okta, third-party identity providers, SaaS applications and cloud environments. It identifies issues such as excessive permissions, dormant identities, configuration weaknesses and other conditions that increase the identity attack surface.

Where licensed and implemented, Principle Networks will use ISPM findings to support proactive identification and remediation of identity security weaknesses rather than relying solely on incidents to expose configuration problems. Principle Networks support you to prioritise findings as part of our Regular Business Reviews according to practical security impact, to investigate identified exposures and coordinate remediation where the affected application platform or Okta configuration falls below your organisations security standards.

Relevant trends and significant improvements to identity security posture can be incorporated into the Regular Business Review so trends towards a more secure identity environment are measured over time.

Privileged Access

Okta Privileged Access provides controls for privileged access to infrastructure and other sensitive resources. Capabilities include access to Windows and Linux servers, management of privileged credentials and service accounts, time-bound access and recording of privileged SSH and RDP sessions.

Where Okta Privileged Access is deployed, Principle Networks support the configuration and operation of the service within the agreed scope, including resource access, policies, assignments and relevant privileged access workflows.

Issues affecting privileged access will be treated with an appropriate operational priority especially where they may prevent administrative access to critical infrastructure, requiring a high priority SLA response.

Principle Networks will work with your organisation to reduce unnecessary standing privilege and maintain a controlled model for privileged access as servers, administrators and operational requirements change.

Access Gateway

Okta Access Gateway allows legacy and on-premises web applications that do not natively support modern federation standards to use Okta authentication. It operates as a gateway between users and protected applications, allowing existing applications to benefit from Okta SSO and authentication policy without requiring significant application redevelopment.

Where deployed, Principle Networks will support the Okta Access Gateway service and associated application integrations within the agreed scope. Operational support is included to investigate issues with availability, authentication and connectivity affecting protected applications.

Secure Partner Access

Okta Secure Partner Access provides controlled access to internal applications and resources for external business partners. It allows 3rd partner user populations to be separated from users part of your organisation and provides delegated administration so that authorised partner administrators can manage defined users and access without requiring unrestricted administrative access to your Okta tenant.

Principle Networks will support the associated partner access configuration, policies and delegated administration model where Secure Partner Access is deployed and in-use.

As partner relationships change, Principle Networks will assist with maintaining the appropriate separation between partner populations, applications and administrative responsibilities. The service helps prevent third-party access from becoming an unmanaged shadow extension of the customer's internal identity environment when engagements come to an end.

Auth0

Auth0 provides Customer Identity and Access Management (CIAM) for applications used by customers, consumers, partners and other external identities. Unlike workforce identity, where an organisation typically controls the user population, devices and access lifecycle, Auth0 is designed to sit within customer-facing digital services where the identity journey forms part of the application experience itself.

The platform enables organisations to provide secure registration, authentication and authorisation across web, mobile and API-based applications, while giving the internal application teams flexibility over how those experiences are presented to different user groups. Auth0 can support traditional username and password authentication alongside passwordless methods, social identity providers, enterprise federation and standards-based integrations such as SAML, OpenID Connect and OAuth. This flexibility allows organisations to offer appropriate authentication methods without having to build and maintain the underlying identity capability independently within each application.

Auth0 can also provide a consistent identity layer across multiple digital services. Rather than separate applications maintaining their own user stores, login processes and security controls, Auth0 centralises many of these capabilities and provide common policies around authentication, session management, Multi-Factor Authentication, federation and access to APIs. For organisations operating several customer-facing platforms, brands or business units, this can help reduce duplicated development effort while creating a more consistent approach to security and identity.

The customer experience is an important consideration within CIAM. Authentication controls must provide appropriate security without introducing unnecessary friction into registration, login or account recovery journeys. Auth0 allows organisations to customise elements such as Universal Login, branding, authentication methods and user journeys so that identity can be integrated into the wider digital service rather than appearing as a separate infrastructure component.

Where Auth0 is included within the managed service, Principle Networks will provide operational support and ongoing management for the Auth0 tenant and the identity components agreed within the service scope. This includes configuration and administration of tenants, Connections, Applications, APIs, Organisations, authentication and MFA policies, Actions, branding and federation integrations.

As part of the Business as Usual service, Principle Networks will investigate federation issues, configuration problems and other tenant-related incidents. This includes reviewing Auth0 logs and authentication events, validating identity provider and application configuration, identifying policy or integration issues and coordinating remediation with your teams where required. As Auth0 is typically integrated directly into application architectures, some incidents may span both the identity platform and the application itself. Where an issue involves application code, SDK implementation, API behaviour or application-side configuration, Principle Networks will work with your development or application teams to help isolate the cause and coordinate resolution.

Ongoing management may also new applications that may need to be onboarded, authentication controls may need to evolve, and existing integrations may require modification as external platforms or application architectures change. Principle Networks will support these changes within the scope of the managed service and ensure that Auth0 configuration continues to reflect the organisation's security, operational and customer experience requirements.

Because Auth0 often provides the authentication layer for externally accessible and potentially business-critical applications, changes require careful control. Principle Networks therefore manages relevant changes with consideration for security, availability and the impact on the end-user journey. In Particular, we are ISO 20000-1 Service Management accredited with a servicedesk that follows an ITIL aligned Change Management Process. These processes will be leveraged across the service, when changes may affect login flows, federation, MFA, Actions, Universal Login and other components that could affect a customer userbase.

Through our managed service, Auth0 is treated not simply as an authentication service but as an important component of the your digital application architecture. Our objective is to maintain a secure, reliable and supportable customer identity platform while allowing application teams to continue developing and evolving digital services without having to take responsibility for the day-to-day operation of the underlying identity platform.

Service Optimisation

Principle Networks will maintain an ongoing understanding of how the customer uses the Okta platform and will identify opportunities to improve security, automation, reliability and administrative efficiency.

This may include simplifying App Sign-In Policies, increasing adoption of FastPass, improving lifecycle automation, reducing direct assignments, improving Group Rules, extending automated provisioning, introducing stronger access governance or making greater use of Okta capabilities not currently implemented by the customer.

Recommendations are driven by our operational experience, as well as periodic assessment. Issues that repeatedly generates support incidents, manual administration or policy exceptions will therefore be considered a candidate for permanent improvement rather than simply continuing to be supported in its existing form. Significant recommendations, trends, risks and improvement activities will be presented through the Regular Business Review where appropriate, providing the customer with an ongoing roadmap for the effective use of their Okta investment.

Configuration Hygiene

An established Okta environment will naturally accumulate configuration as applications, people and business requirements change. Without ongoing management, unused Groups, Group Rules, assignments, policies, mappings, integrations and exceptions can make the environment increasingly difficult to understand and safely modify.

Principle Networks will identify configuration that no longer has a clear purpose, unnecessarily duplicates another control or creates avoidable operational complexity.

This does not mean that configuration will be removed solely because it is old. Principle Networks will establish dependencies and business requirements before recommending rationalisation or change.

Where appropriate, technical debt and significant configuration improvements will be incorporated into the ongoing service improvement activity and Regular Business Review.

Continuous Enhancements

At Principle Networks we like to approach things a little bit differently. We try to put ourselves in a customer's position and understand what we would want to achieve from a service. We used our knowledge of the service and feedback from existing customers to produce a service that delivers on what customers need and want. We incrementally expand and improve our Okta Managed Service to deliver the maximum level of security and value from a customer's decision in selecting Okta as a vendor.

We achieve this through regular engagements, where we do the heavy lifting and allow the customer to make the strategic decisions most appropriate for their organisation.

Regular Business Reviews

A Regular Business Review (RBR) is a regular scheduled meeting or discussion between Principle Networks and your teams provided as part of our Okta Managed Service. The purpose of this review is to assess the ongoing security posture of your Identity Environment, discuss key metrics, address any challenges, and ensure that your organisation is achieving the desired outcomes from their Okta investment and our Managed Service.

Business Update

Principle Networks have a well-defined business review process broken down into key areas.

Service Management Review

During the review we discuss the current level of service and challenges and then dive into the current state of your Okta Identity environment where we can flag any potential issues.

For example:

- We will discuss how well Principle Networks met Service Level Agreement (SLA) Key Performance Indicators (KPIs).
- We will discuss challenges related to the delivery of the Okta service, within the context of your organisation to ensure they are addressed.
- High-risk issues or security cases are discussed.

Security Review

During the meeting we review the organisations information such as new and on-going issues, deployment health and applicable compliance posture, and how that posture can be improved. We will also highlight any changes that may be required and implement them as agreed.

Technology Review

This is a key area of the Regular Business Review, during which an experienced presales or Okta Certified Specialist will talk about a key component of the Okta solution that may already have been purchased but is not currently being leveraged. Although not an exhaustive list, example topics discussed during the technical review have been included in the table below.

Okta Technology Areas (example)
Okta Device Access
Identity Threat Protection
Identity Security Posture Management
Privilege Access
Access Gateway
Secure Partner Access

After a knowledge sharing on the agreed discussion area, we can offer several days professional services to implement the technology and support it as part of the managed service moving forwards.

Further to discussing enhancements and improvements to the Okta Identity Service we end the meeting discussing changes to your business and how that might impact the requirements of your solution and your identity security in general. This is a chance to discuss what is important to you and your organisation and to ensure Principle Networks are ready to help adapt or respond to any challenges coming down the road in a proactive manner.

Service Management

Principle Networks operate under an ISO 20000:1 accredited Service Management System with telephone, email, and web portal access to raise Incident and service requests which are managed against the following target service levels.

Offering	Description
Okta Managed Service	Principle Networks will respond to Service Requests, Change Requests and reports of Incidents submitted by Customers through its Authorised Contacts.
Coverage Hours	24 x 7 x 365
Incident Response Times	Target Response times for Incidents are dependent on the severity level: • P1 - Critical event will be responded within ≤30 Mins. • P2 - Urgent event will be responded within ≤ 30 Mins. • P3 - Important event will be responded within ≤2 hours. • P4 - A request will be responded within ≤4 hours. <i>Please see "Service Levels" section of this document for more detail.</i>
Target Fix Times	Target Fix times for Incidents are dependent on the severity level: • P1 - Critical event, target fix within ≤4 hour • P2 - Urgent event will be responded within ≤8 hours. • P3 - Important event, target fix within ≤32 hours • P4 - A request will be actioned within ≤48 hours. <i>Please see "Service Levels" section of this document for more detail.</i>
Vendor Support Escalation	Principle Networks will escalate items which the Principle Networks Servicedesk team are unable to resolve.

Contacting the Servicedesk

Principle Networks Managed Customers have access to the Principle Networks Servicedesk team. Principle Networks Servicedesk can be contacted as follows:

Contact Method	Details
Email	servicedesk@principle-networks.com
Portal	https://portal.principle-networks.com
Telephone	03330 124 003 (Option 1)

Priority 1 and Priority 2 incidents should be raised via a telephone call to our 24/7 servicedesk number above.

Any fault or service affecting issue will be dealt with by the Principle Networks Servicedesk. Where subject matter experts' input is required, cases will be escalated to the appropriate engineers, 3rd parties or vendors in accordance with prevailing Service Levels. Alternative Service Levels will apply to Change Requests.

Servicedesk Communication and Customer Contacts

Principle Networks Servicedesk communicates with customers through various methods and maintains contact lists with tiers of authority for added security. These contacts can be added to/updated via service request or the customer portal by the named **'Authorised - Including Delegation'**. There are three main contacts that our Servicedesk engineers use to contact customers:

- **Servicedesk Contact** - Is usually a Servicedesk / IT Department distribution list or a named contact who will be contacted by Principle Networks in the first instance.
- **Out of Hours Contact** - Can also be an email distribution list or a named contact who Principle Networks will call/email OOH should this be required.
- **Escalation Contact** - This contact will be used if the Servicedesk and/or OOH contact cannot be reached.

Note: Customer contacts who submit tickets via email or through the customer portal will remain the primary case contact. This can be changed by request, or via the customer portal. In a P1/MSO scenario that is proactively raised by Principle Networks both the Servicedesk Contact and the Escalation contact will be contacted. We recommend that customers use a distribution list (DL) as the primary case contact if more than one person requires updates.

Servicedesk Permissions

For security access reasons Principle Networks has options to set customer permissions for its contacts. These permissions can be updated via service request or the customer portal by the named **'Authorised - Including Delegation'**.

- **Problem Permissions** – Permissions to Raise Problem Cases or Queries.
- **Change Permissions** – Permissions to Authorise or Make Changes, including Service Requests.
- **Options:** **'Authorised'** / **'Not Authorised'** / **'Authorised - Including Delegation'**. *The latter being a management contact who can manage permissions of other contacts within their business E.g. Head of IT, Director)*
- **Maintenance Notifications** – Will receive notifications relating to maintenance/service. E.g. Planned works or Critical Vulnerabilities effecting supported products. *Options: Allow / Do Not Allow*

Note: Should a contact not be authorised to make changes or raise problems, Principle Networks Servicedesk engineers will notify the contact and will request authorisation from a user with **'Authorised - Including Delegation'** permissions.

IT Service Management

The following ITSM processes are implemented:

- Incident Management
- Request Management
- Change Management
- Problem Management
- Configuration Management Database (CMDB) Management
- Continuous Service Improvement

Incident Management

Principle Networks handle Incident Management with precision, adhering to specific Service Level Agreements (SLAs). Each incident is carefully classified and prioritised. Our Servicedesk team then conducts thorough investigations, diagnoses the issue, and ensures swift resolution with root cause, all in accordance with our ISO 20000:1 service management standard.

P1 and MSO Process

Principle Networks have internal Priority 1 incident and major service outage processes to tackle those incidents that need urgent attention.

Request Management

Customers can make service requests in relation to their Principle Networks managed service. For example, ask question about their service or user creation.

Where a request type is deemed as a chargeable requirement the customers Change Hours Contract can be used for professional services time. Should a request fall out of scope of a Change Hours Contract then the request will be passed on to the customer's account manager to progress as a project.

There are two case types that Principle Networks use within our IT Service Management (ITSM) System to categorise service requests; these are:

Query – A query can be a question or request for information about a customer's existing service or a service a customer may want to consume. Often queries develop into a change request or a referral to the customer's account manager should any further actions be required such as scoping requirements for a project.

Service Request – Is a formal low risk request for something to be provided. For example, this could be a password reset, or a new user request. These requests a low impact changes that are quick to action which save the use of having to go through the change management process.

Change Management

All changes will be categorised as a change request within with Principle Networks ITSM system and will be sub categorised as Standard or Normal changes. Either change can be assigned a priority level between P1 (Emergency) and P4.

All changes are chargeable with time taken from the customer Change Hours Contract, as described within this document. Changes adhere to Principle Networks' standard Service Levels defined within this document. As standard, all changes are prioritised as P4 and completed in hours as defined in the SLA.

Changes may be completed out of hours at customer request when Principle Networks resource is available. Out of hours change time is taken from a customer Change Hours Contract at double time.

Multiple changes of the above types or those that are estimated to take longer than 4 hours could be seen as a larger piece of work. Where this is the case, the request would be directed through to an account manager to produce a scope of works and will be chargeable based on the scope.

Change Request Authorisation

To ensure security and accountability, all change requests must be submitted by an authorised representative from your organisation. This representative must be pre-approved by an 'Authorised - Including Delegation' contact, as defined on page 6. Typically, these individuals hold key roles such as IT Director, IT Manager, or an equivalent position. The 'Authorised - Including Delegation' contact is responsible for owning and maintaining the list of approved contacts who are permitted to request or approve changes. For added security, Principle Networks securely stores these authorised contact details within our ITSM system, ensuring that only verified personnel can initiate or authorise change requests.

Standard Change Request

Standard Changes have been defined as a '**Business as Usual**' task and do not follow the full normal change management process. All standard changed requests will be given the P4 SLA.

A Standard Change request is categorised as a low risk / low impact change which is usually commonly requested and frequently implemented. They follow company work processes where appropriate and have a proven history of success.

Types of changes covered by a standard change (Subject to complexity) example are:

- **Cloud Configuration Change**
- **Security Policy additions**
- **Access Policy Creation or Change**

Normal Change Request

Normal change requests are considered those that do not fall into any standard change category. The impact is often moderate to very high and holds a medium to very high risk. Formal procedures must be followed to ensure that each step of a normal change request case is completed in line with this process.

Every normal change must undergo a detailed review of the customers requirement which comprises of:

- **Change Reason and Justification**
- **Change Details and Associated Equipment**
- **Post Change Test Details**
- **Impact Analysis, Highlighted Risks and Mitigation**
- **Rollback Details**

Emergency Change Request

The emergency change process is in place to work around or resolve high impact and high-risk incidents that are causing substantial business disruption. An Emergency Change could also be utilised to protect the customer's business from threats such as are likely to result in an incident if not addressed promptly, for example a critical security vulnerability that could result in a cyber-attack. Emergency changes follow the incident management P1 process and maintain the standard case type of '**Change Request**'.

Problem Management

Principle Networks follows a robust and structured Problem Management process designed to identify, investigate, and resolve the root causes of recurring or major incidents. This process ensures minimal disruption to services and supports continuous improvement in line with best practices. Our approach aligns with the Problem Management guidelines audited and certified under ISO/IEC 20000-1, ensuring compliance with international standards for IT Service Management. Through proactive and reactive problem management, we deliver consistent, high-quality outcomes for our clients.

Proactive Monitoring

Principle Networks provides comprehensive proactive monitoring across all supported Okta services to ensure the security of your Identity environments. Monitoring activities focus on the issues that occur within your Identity environments as well as monitoring of the service's health to ensure that your environment is continuously assessed and new issues detected and addressed.

Principle Networks predominantly leverage Okta's alerting capabilities to integrate with our ITSM and raise cases automatically on your behalf. These cases are assigned and investigated to understand the scope of the issue, before contacting your teams directly to discuss the issue and put a plan in place to remediate any issues.

Note that with your agreement, Principle Networks may also interrogate your Okta environment using Okta's API using read-only credentials to more quickly identify problems and pro-actively respond to issues where alerting alone may not be appropriate.

Low-Priority Issues

Principle Networks will not typically create cases proactively for low-priority issues due to the number involved and the 'noise' these issues would create for your teams. Low-priority issues will instead be discussed during Regular Business Reviews once outstanding higher priority issues have all be resolved and Change Requests to resolve them created and implemented as agreed.

Principle Networks can respond to Low-priority issues as well if this is more appropriate for your organisation but please note the use of Change Hours usage may grow significantly and result in requiring an increase in contracted hours.

Continuous Service Improvement (CSI)

At Principle Networks, we are committed to continually enhancing and evolving our services. We actively collaborate with our customers, encouraging feedback on our performance and identifying opportunities where we can add greater value and make meaningful improvements.

We encourage feedback after closure of every service case and all feedback is reviewed. Feedback can be about the service, a service feature request or feedback to an individual Servicedesk engineer. Improvement suggestions and feature requests will be added to Principle Networks continuous service improvement (CSI) register and will be reviewed regularly. Strategic focus for service operations is defined by what can be achieved through our continuous service improvement program.

Change Hours Contracts

Except for patching for high or critical vulnerabilities, Principle Networks does not include any other changes within the standard service. For other changes, we offer Change Hours Contracts as a flexible solution, allowing customers to incorporate change requests into their Managed Service contract. This can be arranged as part of a monthly allowance or purchased on an ad-hoc basis, depending on the customer's preference.

Change Hours Contracts may only be utilised for change and works in relation to services Principle Networks support, unless explicitly agreed. They may not be utilised for break fix or high-priority problems and faults and are handled through the Managed Service for supported solutions.

Time is recorded for all work in increments of 30 minutes; thus, this is the minimum amount of time per change. Anything that is estimated to take over 4 hours or more may be classed within a project scope and will need the appropriate resource assigned to fulfil the requirement and may require a full scope of works and/or project management and may be charged against a separate quote signed by the customer.

Customers have the option to purchase monthly hours that can be used for ongoing service and change. Monthly hours top the customer's recurring hours back to the contracted value of the 1st of each calendar month. Hours not used within the calendar month are lost.

Additionally, there is the flexibility to buy a bank of non-recurring hours, which serve as a reserve that can be utilized as needed. This system provides a convenient way to manage time allocation for services, allowing customers to plan and budget their support needs effectively.

If more time is used in a month than what is contracted, the excess time will be deducted from the non-contracted 'bucket'. If there is no time available in the non-contracted bucket, overuse will result in a negative balance. Any underuse in subsequent months will then reduce this negative balance until it is eliminated. If overuse continues to accumulate, your account manager will reach out to discuss increasing the contracted amount or potentially introducing a hard limit to prevent further overuse of Change time and avoid additional charges.

A monthly report is available to customers to detail hours used and highlight the remaining Change Hours allowance. This can be enabled by the customer through the Principle Networks Portal or by raising a service request with servicedesk@principle-networks.com.

Note: Change Hours are billed at double the standard rate for out-of-hours (OOH) services. If hours extend into arrears, customers may be required to either pay for the additional time used over the agreed contract or modify their existing agreement to accommodate the increased use of the service. This revision aims to clarify the billing practices for Change Hours and the options available to customers should they exceed their allocated hours.

Ad-Hoc Service Reporting

High-Level Ad-Hoc Reporting Upon Request (Service Request): Customers can request service reports, including availability, incident counts, and SLA adherence, through a service request. The service management team will generate these reports tailored to the customer's specific needs.

Please note that this service may incur charges, which will be deducted from the customer's Change Hours Contracts. For comprehensive service management solutions, Principle Networks provides a dedicated service. For more information, customers are encouraged to reach out to their respective account manager.

Principle Networks Customer Portal

Customers are invited to request access to the Principle Networks customer portal. This portal allows you to track your support tickets, view contracts, and update company contacts. To gain access, please email servicedesk@principle-networks.com. You must be a designated change authority for your organisation, or alternatively, an authorised contact within your company can request access on your behalf.

An existing portal user from your organisation with admin rights can also provide you with portal access by assigning your portal role from the User Management page.

24x7 Service Operation

Managed customers benefit from 24/7 Servicedesk access, ensuring they receive prompt assistance for high-priority incidents or emergency changes. It is important to note that customers need to initiate a phone call to request this level of support. For detailed definitions of each priority level, customers should refer to the Service Level Agreements (SLAs) provided in the appendix of the document. This structure helps maintain an efficient and responsive support system.

Note: Principle Networks collaborate and support your organisation's IT and servicedesk teams, so 1st and 2nd line support for end users within your organisation is still a requirement

Access to 3rd line engineers

Principle Networks ensures that their managed customers have direct access to 3rd line engineers. To delve into what this means:

- **Expertise** - When you encounter complex technical challenges, our senior engineers bring a wealth of knowledge, skills, and experience to the table. Our engineers swiftly analyse issues, propose solutions, and guide your team effectively.
- **Speed** - The service operations are automated and technology-driven, ensuring optimal efficiency, saving valuable time and money. When critical incidents arise, our engineers respond promptly, minimising disruption and downtime.
- **Quality** - Principle Networks adheres to best practice service management standards. Our 3rd line engineers maintain consistency, ensuring high-quality support and governance.
- **Assurance** - With industry-leading Service Level Agreements (SLAs) and proactive support, you can trust that any network issues will be resolved rapidly, minimising impact on your operations.

Principle Networks' 3rd line engineers play a crucial role in maintaining reliable, secure, and high-performing networks.

Co-Management Arrangements

Administrative access to Okta provides significant control over authentication, applications, users and security policy and therefore requires stronger governance than standard user access.

Principle Networks will support and manage your Okta administrative model with you. Including Standard Administrator Roles, Custom Admin Roles and Resource Sets where these are used. Administrative changes and access-related issues will be investigated as part of the managed service where appropriate. Principle Networks maintain oversight of the number and type of highly privileged administrators and identify opportunities to replace broad permissions with more targeted administrative roles. API tokens, OAuth-based administrative integrations and other administrative dependencies will be considered where they form part of the managed solution. The objective is to maintain sufficient administrative access to operate the platform while avoiding unnecessary standing privilege or reliance on individual administrators.

As part of co-management customers are free to manage their own internal change process or are welcome to use Principle Networks to peer review or as an escalation point for changes where appropriate. We anticipate customers having full access to their Okta Identity environment and we expect our teams to work together on identified issues and agree ownership such as where you leverage our team to remediate it or decide to complete the resolution internally.

It is the customers responsibility to ensure any changes they make have been verified and tested prior to implementation to ensure no unanticipated downtime to their network services. We strongly recommend customers utilise their own UAT plans (user acceptance testing) after each change. Should any support on changes be required it is advised that customers log the change request to the Principle Networks Servicedesk for the team to verify and support the change.

Escalation and Management

Any service partner or hardware vendor escalations will be managed by Principle Networks as an integral part of our service. Our commitment extends to ensuring seamless communication and resolution with external partners.

Comprehensive vendor support applies only to Principle Networks managed services. In cases where a service is unmanaged, the responsibility for escalations lies solely with the customer.

Principle Networks Escalation

For customers wanting to escalate a part of their Principle Networks service the process can be found in the appendix of this document.

Service Levels (SLAs)

Principle Networks Managed Services are monitored 24 x 7 x 365. Within contracted support hours, Principle Networks will respond to autogenerated cases raised by the monitoring systems or to cases raised by the customer within the Service Level Agreement terms.

See the below the description of Service Level against the target response and resolve times:

Priority	Description
P1	A Critical business service is non-operational impacting the customer organisation, multiple users, or multiple sites; or Severe functional error or degradation of service affecting production, demanding immediate attention. Business risk is high, with immediate financial, legal, or reputational impact.
P2	The client is experiencing failure or performance degradation that severely impairs operation of a critical business service; or the client or service has been affected, although a workaround may exist; or Application functionality is lost; or significant number of users or major site is affected. Business risk is high.
P3	The client is experiencing a problem that causes moderate to low business impact. The impact is limited to a small number of users; or incident has moderate, not widespread impact; or the customer or service may not have been affected. Business risk is low.
P4	Standard service request; Change request; Enquiry; or updating documentation; system patch or upgrade. Low or Minor localised impact.

The following table describes the target response and fix times for the levels of service for incidents raised.

Priority	Target Response Time	Target fix time *	Working time
P1	30 minutes	2 hours – resilient solution 4 hours – hardware replacement 5 hours – leased-line connectivity	24 hours, 7 days a week, 365 days a year
P2	30 minutes	8 hours	24 hours, 7 days a week, 365 days a year
P3	120 minutes	32 hours	Monday – Friday 8am – 5:30pm
P4	240 minutes	48 hours	Monday – Friday 8am – 5:30pm

***Target fix times may be limited by 3rd party providers and their associated SLA, which may hinder Principle Networks ability to fully restore service.**

Fault Resolution

The Fault Resolution measures apply to Incidents which represent a Service Failure. The duration of a Service Failure and related target maximum Resolution Time is measured, during Contracted Hours, from the point at which the Customer or Principle Networks register the fault within Principle Network's IT Service Management (ITSM) to the point at which Service Failure is no longer present.

Fault Response and Resolution

Principle Networks shall endeavour to respond to and resolve Service Failures within the Response Times and the Target Resolution Times stated above. If it is identified during fault investigation that due to circumstances beyond Principle Networks control, restoration times will exceed the stated target Resolution Times, the Customer will be notified. Principle Networks shall not be liable to the Customer should the Response Times and Target Resolution Times not be met.

Escalations Process

Please raise your escalation by emailing directly to the intended recipient and cc any relevant parties. All previous correspondence should be included. Also please note that when the next escalation has more than one contact, all parties should be included.

Our escalations contacts can also be reached by phone call. If the contact is unavailable, please leave a message and wait for their reply. In the absence of any contacts listed, please be directed to the secondary contact stated in their out of office message.

Should you not receive an acknowledgement to your escalation within the stated timeframe, please escalate to the next level.

A service case priority level is agreed between the customer and Principle Networks when the initial call is raised. The priority level of a given case may be increased by the customer due to a change in circumstances or the amount of time elapsed during the support process. Should a customer feel a case is not being handled as expected the following escalation paths can be followed and available 24/7, also known as a hierarchical escalation:

Escalation Level	Contact	Telephone	Email
Level 1	Servicedesk Lead	07399 329 504	adnan.fatah@principle-networks.com
Level 2	Head of Operations	07572 160 006	richard.tm@principle-networks.com
Level 3	Co-Chief Executive Officer	07738 022 937	alex.steer@principle-networks.com

Complaints Process

Principle networks takes great pride on delivering an exceptional service to its customers. Should a customer feel that Principle Networks high standards have fallen short of their expectation the customer should contact the head of operations by email at:

richard.tm@principle-networks.com

Upon receipt of correspondence from the customer, Principle Networks will respond to the customers complaint within (5) business days.