Principle Networks

Service Description - Wiz Managed Service

Contents

Introduction

This document describes the Wiz Managed Service, service levels and enhanced options provided by Principle Networks. This Service Description applies specifically to Principle Networks' **Wiz 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 Wiz Partner and Wiz Managed Service (MSP) Partner.

Wiz 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 as part of any Wiz licensing ordered. 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	Managed Service	Enhanced Options
Specialised Wiz Support	✓	
Continuous Enhancement	✓	
Regular Business Review	✓	
Cloud Security Posture Management (Essentials or Advanced)	✓	
Cost Savings Identification	✓	
Data Security Posture Management		✓
Compliance Framework Reporting and Improvements		✓
Runtime Workload Protection (Wiz Sensor)		✓
Code Security (Wiz Code)		✓
Cloud Threat Detection and Response (Wiz Defend)		✓
Virtual Machine Patch Management		✓
Service Management	✓	
Deployment Health Monitoring	✓	
Change Hours Contracts		✓
Ad-Hoc Service Reporting	✓	
Principle Networks Customer Portal Access	✓	
24/7 Servicedesk	✓	
Access to 3rd Line Engineers	✓	
Co-Management Arrangements	✓	
Escalation Management	✓	
Maintenance Notifications	✓	

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

Principle Networks Ltd | Head Office: The Stanley Building, 7 Pancras Square, London, United Kingdom, N1C 4AG
Reg No: 11341216 | Registered in England & Wales | VAT No: 294928252

Wiz Managed Service

The current cloud security landscape is shaped by speed and sprawl. Organisations are deploying more services across Azure, AWS, Google Cloud and Kubernetes, often with multiple accounts/subscriptions, and with constant change through Continuous Integration / Continuous Delivery. This pace creates three common challenges.

1. **Visibility gaps where teams or senior management don't fully understand what exists and where.**
2. **Misconfiguration and privilege creep, the default cause of exposure.**
3. **Alert overload with many findings and not enough context to know what matters.**

On top of these, attackers increasingly target identity such stolen tokens/keys, compromised service accounts and exploit a combination of issues less critical in their own right. These create toxic combinations which cause very real exposures and can lead to a data or security breach. Wiz is designed to address these challenges by focusing on rapid, broad coverage and contextual prioritisation of issues through analysis of their combined impact to attack paths.

At Principle Networks, our goal is to leverage Wiz Cloud to mitigate security issues impacting your cloud environment and use the plethora of capabilities within the Wiz Cloud to maximise your organisation's investment in Wiz.

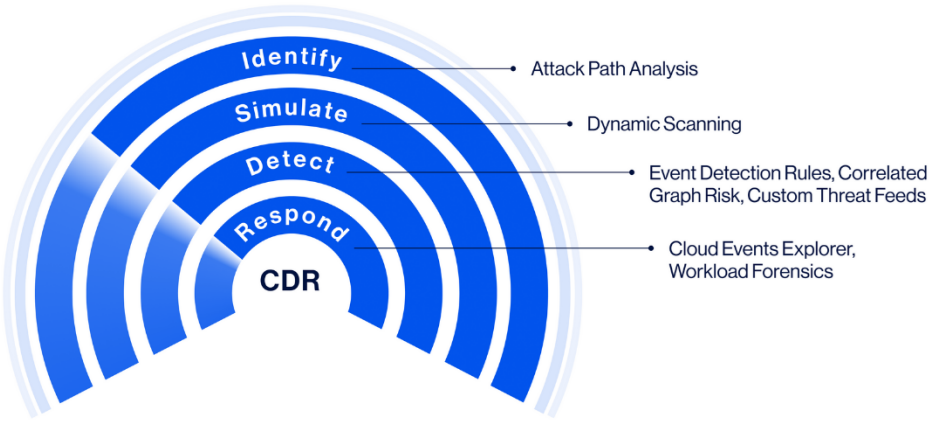
We provide a full or co-managed Wiz service designed to meet the specific cyber security needs of organisations on their cloud adoption journeys. We handle the deployment health, management, operation, identification of cost savings and support of Wiz state-of-the-art Cloud Security solutions, keeping your organisation environment cloud fully monitored and always protected while you and your teams are able to access your Wiz Cloud, either to collaborate with us on addressing issues, or for your own specific requirements.

Principle Networks Ltd | Head Office: The Stanley Building, 7 Pancras Square, London, United Kingdom, N1C 4AG
Reg No: 11341216 | Registered in England & Wales | VAT No: 294928252

What is Wiz?

At its core Wiz is a SaaS based cloud platform that offers several products to addresses various cloud security and data issues. Wiz evaluates cloud configurations across environments to highlight risky cloud configurations such as public exposure, insecure storage, weak network controls, and deviations from security baselines. This addresses configuration drift that comes from frequent changes and decentralised cloud ownership.

One of the biggest challenges in cloud security is not knowing what's running or how it connects. Wiz builds a unified view of cloud assets (workloads, services, identities, data stores) and their relationships, which supports governance, incident triage, and day-to-day risk management.



A major challenge is prioritising vulnerability work. Traditional scanning can produce thousands of CVEs with little clarity on exploitability. Wiz's workload and vulnerability context links vulnerabilities to real exposure conditions such as whether the workload is internet-facing, what permissions it has and what sensitive data it can reach. It automatically contextualises the risks and determines whether there's an accessible route through an attack chain that can result in a breach. This consolidates thousands of vulnerabilities into a handful of clearly prioritised issues that tell your teams and ours exactly what we need to focus on first.

Cloud Security Posture Management (CSPM)

Cloud Security Posture Management (CSPM) is the heart of Wiz Cloud. Wiz's CSPM capability continuously assesses all of your cloud environments (such as Azure, AWS and GCP) for misconfigurations and policy drift across services like identity, networking, storage, logging, and encryption. Wiz pulls in cloud configuration data and normalises it into a single view, then maps issues to risks and compliance requirements so we can focus on what genuinely increases your organisation's exposure, such as publicly reachable services, overly permissive access, and missing protective controls. Instead of producing a long checklist, Wiz's CSPM capability helps us explain why something matters by showing how a misconfiguration contributes to an attack path and what it could impact or expose.

Principle Networks teams use Wiz's CSPM findings to identify risks to your organisation through consistent outcomes. We proactively respond to alerts generated by Wiz, triage, assign and track issues against our defined Service Level Agreements (SLA) without flooding your cloud and security teams with noise. Principle

Networks servicedesk work with your teams to review new and changing risks, prioritise them by impact, and produce clear remediation actions. Where required we produce detailed Change Requests for your cloud environments for your teams to review and action, or we can action them on your behalf during an approved maintenance window as part of a Change Hours Contract, also described later in this document.

By investing in a Principle Networks Wiz Managed Service, you can be confident that new and existing security issues within your cloud environment are being proactively raised and progressed to resolution, while we remove the leg work for your teams so they can be less reactive and spend more time delivering value for your organisation.

Where it is agreed that Principle Networks can access your cloud environment to review configuration and remediate cloud configuration issues with your approval as part of our Change Process, we highly recommend using Privilege Identify Management (PIM) and Just In Time (JIT) access. This ensures that privileged roles are managed via approval workflows with necessary justifications, and that assigned roles are automatically removed after a period of time. This greatly reduces the attack surface created by users with privilege access and roles and can also be utilised internally for your teams in the same manner. This can be designed and configured as part of onboarding where defined and scoped during the sales process, or as a separate piece of scoped work at any point during the life of your Managed Service. Please speak to your account manager for more information.

Cost Savings Identification

The nature of Wiz Cloud's solutions results in it collecting a full database of all your organisations cloud resources and how they are associated to one another. The information stored within Wiz provides the ability for us to leverage that data in ways that can achieve customised objectives.

As part of our managed service, Principle Networks produce a number of reports that can identify cloud resources that may no longer be in use but are still costing your organisation money. These reports can be tuned as part of the managed service but broadly can identify areas such as orphaned resources, including disks, public IPs, VPN and Network Gateways, etc, that are not associated to other resources and so not currently in active service but have an on-going cost. We also report on disabled resources such as powered off Virtual Machine and Network Virtual Appliance (NVA) instances that may have been decommissioned but not deleted.

Our cost analysis provided as part of our Wiz Managed Service can result in significant cloud cost saving on day one and provide budget owners piece of mind ensure that costs are accurate and that cloud sprawl doesn't result in operational expenditure creep.

Data Security Posture Management (DSPM)

Wiz's Data Security Posture Management (DSPM) is an additional license option that answers three practical questions.

- **Where does your sensitive data live?**
- **Who can access it?**
- **How could it become exposed?**

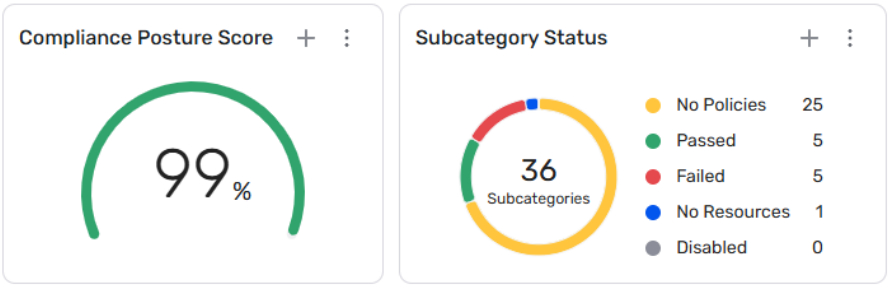
Wiz's DSPM module works by discovering and classifying sensitive data across common cloud data stores (for example buckets, volumes, and databases) using built-in classifiers for regulated data types like PII and PCI, as well as custom classification rules where needed.

Wiz correlates this data with context against cloud risks just like CSPM and is able to correlate misconfigurations, identity permissions, and workload exposure to highlight the scenarios that require attention such as a sensitive dataset that is publicly accessible through a 'toxic combination' of permissions and exposure.

Wiz Cloud is built around a unified risk model, so DSPM findings aren't isolated data alerts. They're connected to the owning resource, identity and pathway like any other issue identified by Wiz Cloud. This enables our teams to prioritise and highlight new DSPM issues and produce remediation steps via our Change Process at pace, in the exact same manner as for CSPM.

Compliance Framework Reporting and Improvements

All organisations have a degree of security compliance they must adhere to in order to demonstrate to external parties and authorities their adherence to good cyber security health and security best practice. Wiz supports organisation's security compliance in an on-going basis by analysing policies, threat and issues against a large number of Frameworks.



As part our Wiz managed service where agreed during the sales process, Principle Networks will report the organisation's cloud infrastructure compliance against applicable frameworks as part of our Wiz Business Review (WBZ) and subsequently work with you and your teams to address shortcomings via our Change Request process. This on-going enhancement service not only drives your organisation towards a better security posture but also focuses efforts to reduce reactive administrative works during audits.

Please note that while Wiz supports many different frameworks, the frameworks relevant to your organisation must be confirmed as supported as part of the sales process. Additionally, Wiz can only report on items that Wiz can attest to, such as technical controls. Wiz cannot audit organisational policies for example so should not be considered as a full compliance audit for any framework.

Runtime Workload Protection (Wiz Sensor)

Wiz Sensor is an optional licensed capability that provides lightweight runtime component, adding kernel-level visibility where agentless snapshots and logs can't fully explain "what's happening right now?". Wiz Sensor's extended Berkeley Packet Filter (eBPF) is designed for Linux and Kubernetes and can be deployed so one sensor monitors all containers on a node, avoiding heavy per-container agents.

In the current threat landscape where attackers chain identity misuse, living-off-the-land activity, and container escape attempts, runtime telemetry is crucial. The Wiz Sensor captures deep execution signals (process, syscall and network-style activity) to enable runtime threat monitoring, file integrity monitoring, and drift detection, and can support real-time blocking/containment as part of Wiz Defend.

Importantly, the sensor's findings are enriched with Wiz Security Graph context (code-to-cloud relationships, exposure, identities, and data), which helps reduce noise and speeds up investigation and response by showing impact and blast radius, not just an isolated alert.

Code Security (Wiz Code)

Wiz Code is an additional licensed application security capability that helps Development catch and fix cloud risks before they reach production. Wiz code scans developer-facing inputs like Infrastructure as Code (IaC), application dependencies, container artifacts, secrets, and CI/CD configuration, then connects those findings to real cloud exposure using code-to-cloud mapping. It has been built to address today's main application security challenges, lots of automated findings with unclear priority, misconfigurations that get deployed at speed, with a disconnect between what security sees in the cloud and what developers can change in the repos. Wiz Code traces critical cloud risks and attack paths back to the exact source code and owner and can surface guidance directly in places developers work (IDE/PR/CI).

Principle Networks will ensure cloud code repositories are correctly onboarded and their Wiz deployment monitoring heath is maintained. Our teams will respond to issues arising due to developer code or the use of outdated libraries and repos they may not be aware have vulnerabilities. Our teams will work with your development teams to identity the root cause of issues identified in order for them to remediate security exposures.

Please note that Principle Networks will not provide or enact updates to your code base.

Cloud Threat Detection and Response (Wiz Defend)

Wiz Defend is an optional cloud detection and response capability, built for runtime threat detection, investigation, and response across cloud environments. It addresses Security Operations (SecOps) challenges in the cloud, limited runtime visibility across fast-changing workloads, noisy alerts that lack cloud context, and attacks that chain together identity misuse, control-plane changes, and workload activity into a single breach path.

Wiz defend provides protection to detect, investigate and respond to issue in real-time when the traditional risk exposure from agentless scanning isn't acceptable to production environments. Principle Network's support teams dove tail into this offering by responding to issues raised by Wiz defend within SLA backed response times to ensure that security issues identified with your workloads and resources at responded to immediately and resolved.

When a threat issue is raised, Wiz Defend already has it enriched with runtime signals via the eBPF-based Wiz Sensor, cloud/SaaS telemetry and Security Graph context. These enrichments make the response decisions significantly faster and safer, delivering a substantial reduction in Mean Time to Repair (MTTR).

Note that agentless Wiz environments without Wiz Defend licensing operate on a 24 hour scan schedule to identify new issues.

Virtual Machine Patch Management

After cloud configuration issues, vulnerability OS and applications are the primary cause of cloud infrastructure becoming compromised. With this enhanced option, Principle Networks' Servicedesk team will take on responsibility for applying patches to Linux and Windows operating systems to mitigate issues caused by software vulnerabilities, as opposed to merely flagging that a patch is required to remediate an issue. This task is performed proactively in accordance with our change management procedures during pre-agreed maintenance windows, typically on a weekly basis. Our proactive approach to patch management ensures the ongoing security of your cloud is managed before critical exposure issues arise.

Principle Networks don't currently offer tooling to monitor and manage the patching of Kubernetes beyond the OS that they reside on where applicable. This limitation affects control plane, Kubelet/Kube-proxy versions or cluster add-ons. Where this is of interest to your organisation, please reach out to your account manager who can investigate possible options to achieve your requirements.

Principle Networks Ltd | Head Office: The Stanley Building, 7 Pancras Square, London, United Kingdom, N1C 4AG
Reg No: 11341216 | Registered in England & Wales | VAT No: 294928252

Specialised Support

We understand Wiz's solution offering intimately and have a proven record of accomplishment with customers for delivering excellent solutions with Wiz while delivering confidence that they are 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 will add security policies and controls to the customer cloud tenants. With customer approval, our engineers can produce Change Requests that are reviewed and approved internally before being sent to you for your own internal review and approval and implement the Change within your cloud environment at a window agreed by you.

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 the Wiz service to deliver the maximum level of security and value from a customer's decision to select Wiz 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.

Wiz Business Reviews

A Wiz Business Review (WBR) is a regular scheduled meeting or discussion between Principle Networks and your teams provided as part of our Wiz Managed Service. The purpose of this review is to assess the ongoing security posture of your Cloud environments, discuss key metrics, address any challenges, and ensure that your organisation is achieving the desired outcomes from their Wiz 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 their Wiz 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 Wiz 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 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 Wiz Certified Specialist will talk about a key component of the Wiz 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.

Wiz Technology Areas (example)
Security Compliance Framework
Shadow Data Management
Cloud Cost Management
Code Security (Wiz Code)
Cloud Threat Detection and Response (Wiz Defend)
WizOS

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 Wiz Cloud service we end the meeting discussing changes to your business and how that might impact the requirements of your solution and your cloud 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
Network 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. ***Please see "Service Levels" section of this document for more detail.***
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. ***Please see "Service Levels" section of this document for more detail.***
Vendor Support Escalation	Principle Networks will escalate items which the Principle Networks Servicedesk team are unable to resolve.

Contacting the Servicedesk

Principle Networks Managed Network 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

Principle Networks Ltd | Head Office: The Stanley Building, 7 Pancras Square, London, United Kingdom, N1C 4AG
Reg No: 11341216 | Registered in England & Wales | VAT No: 294928252

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 onto 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 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 give 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 either a 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 Wiz services to ensure the security of your Cloud environments. Monitoring activities focus on the security issues that occur within your Cloud environments as well as monitoring of the deployment health to ensure that your resources are being continuously assessed and new issues detected.

Deployment Health

Principle Networks create integrations between your Wiz cloud environment and our ITSM tools to ensure that servicedesk cases are created automatically when one or more of your Wiz deployments becomes unhealthy to ensure all cloud resources are monitored and maintained. As part of the deployment and service onboarding we will create automation rules to ensure the baseline health monitoring is in place.

- **New deployment health issues**
- **Unscanned compute assets**
- **Unscanned Storage resources**
- **Missing Kubernetes sensors**
- **Failed cloud integrations**
- **Stale scan data over threshold**

Security Issue Detection

New security issues are reported to Principle Networks ITSM tools and servicedesk cases created automatically whenever a new Critical, High or Medium Wiz issue is detected. The issues will be prioritised in the following manner with the appropriate SLA assigned based on the Service Levels section in this document.

Wiz Issue Priority	Principle Networks Priority
Critical	P2
High	P3
Medium	P4

A specialist Wiz consultant will review the case details and access your Wiz environment to analyse the issue before contacting your teams to discuss it and identify whether any remediation is required to resolve it. Remediation will be completed as part of our Change Request process defined earlier in this document.

Low Priority Security 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 Wiz Service 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 is 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 efficiency and saving valuable time. When critical incidents arise, our engineers respond promptly, minimising 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

Principle Networks provide customers with a tiered co-management access (vendor supporting), this can be restricted to a level to allow customers to undertake minor changes or complex changes depending on their requirements and experience. 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 Wiz Cloud 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.

Maintenance Notifications

Principle Networks work with several service partners who from time to time perform planned maintenance to continuously improve the stability of their products and services. Using downtime schedules Principle Networks ensure that any notification of planned works that they receive that is service affecting will be added to a downtime schedule and a calendar invite will be sent to the selected maintenance contacts to ensure the customers are kept informed of all planned works.

Customers can request maintenance notifications by emailing the servicedesk@principle-networks.com and raising a service request. Notifications can also be stopped using the same method.

Customer Maintenance

It is the customers responsibility to notify in advance any planned work taking place that may affect the security alerting of the managed service supported by Principle Networks. A downtime schedule will be created for the date/time of the work, and a description will be added including the case number to ensure all parties are aware.

The downtime schedules ensure that alarms are suppressed for the duration of planned work. Once the end date and time has lapsed alarm suppression is lifted automatically and normal service monitoring of the solution is resumed.

False alarms resulting in a pro-active response to the issue by Principle Networks caused by customer maintenance not communicated in advance may be deemed chargeable or recorded against the customer's Change Hours Contract.

Principle Networks Ltd | Head Office: The Stanley Building, 7 Pancras Square, London, United Kingdom, N1C 4AG
Reg No: 11341216 | Registered in England & Wales | VAT No: 294928252

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.

Principle Networks Ltd | Head Office: The Stanley Building, 7 Pancras Square, London, United Kingdom, N1C 4AG
Reg No: 11341216 | Registered in England & Wales | VAT No: 294928252

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.