Principle networks

Service Description

Cloud Managed Service

Table of Contents

Introduction

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.

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

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

Cloud Managed Service Overview

Principle Networks will offer the following as part of the managed service, enhanced options are available to add-on to the service:

Service	Managed Service	Enhanced Options
Service Management	✓	
Pre-Paid Days Contracts		✓
Ad-Hoc Service Reporting	✓	
Monitoring Platform Access	✓	
Customer Portal Access	✓	
Azure Health - Cost management	✓	
Azure Health - Security	✓	
Azure Health - Reliability	✓	
Azure Health - Operational Excellence	✓	
Proactive Monitoring Minor/Alert (8-6)	✓	
Proactive Monitoring Critical/High (24/7)	✓	
24/7 Servicedesk	✓	
Access to 3rd Line Engineers	✓	
Patch Management (High/Critical Vulnerabilities)	✓	
Patch Management (Non High/Non Critical Vulnerabilities)	✓	
Certificate Management	✓	
Co-Management Arrangements	✓	
Escalation Management	✓	
Maintenance Notifications	✓	
Vulnerability Scanning of Internet Facing Appliances	✓	
Backup / Configuration management		✓
Azure Site Recovery		✓
Business Continuity & DR Testing		✓
Microsoft Entra ID Identity & Access Management		✓
Microsoft Intune Mobile Device Management (MDM)		✓
Platform Automation and DevOps		✓
External Vulnerability Testing		✓
Business Review (Service Management Review)		✓
Cloud Firewall Review		✓

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

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

Contact Method	Details
Email	Servicedesk@prinviople-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

Principle Networks Servicedesk has various methods whereby it communicates to customers. These contacts can be updated via service request or the customer portal by users with '**Authorised - Including Delegation**' permissions. 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 in the event that 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.

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 standards.

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 such as on the monitoring portal or a VPN account.

Where a request type is deemed as a chargeable requirement the customers pre-paid days contract can be used for professional services time. Should a request fall out of scope of a pre-paid day's 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 pre-paid days 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 pre-paid days 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 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):

- System reboot
- Security Policy additions
- Cloud Network Changes such as UDR and NSG modification
- Existing VPN Configuration
- OS Patching and Firmware Upgrades
- Load balancer Rules
- Instant Resizing
- User Management

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 Assets
- 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.

Configuration Management Database

The Configuration Management database (CMDB) underpins all ITSM services and provides the data required for effective Incident, Request, Change and Problem Management. Principle Networks CMDB holds information about all supported assets and services such as virtual machines, App Services, NVAs and firewalls and holds key pieces of information about them such as device name, site locations, management IP address information, product types, serial numbers and software version.

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 mainly defined by what can be achieved through our continuous service improvement program.

Pre-Paid Days Contracts

With the exception of patching for high or critical vulnerabilities, Principle Networks does not include changes within the standard service. For other changes, we offer pre-paid day 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.

Pre-paid days 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 of the monthly allowance in subsequent months will reduce any negative non-contracted balance until it is eliminated. If overuse on the non-contracted valance 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 pre-paid days allowance. This can be enabled by the customer through the Principle Networks Customer Portal or by raising a service request with servicedesk@principle-networks.com.

Note: Pre-paid day time is 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 pre-paid time 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 pre-paid days 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**.**

Monitoring Platform

Customers can request Read-Only access to the Principle Networks monitoring platform. If you wish to obtain access, please send an email to servicedesk@principle-networks.com. Please ensure that you are a designated change authority for your company, or have an authorised contact within your company submit the request on your behalf.

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.

Proactive/Reactive Monitoring of Solution and Services

- Proactive Monitoring for Critical/High Alerts - Available 24/7
- Proactive Monitoring for Minor/Trouble Alerts - Operational from 8 AM to 6 PM

Principle Network's monitoring platform diligently tracks availability around the clock, every day of the year. Customers may request access to this platform to examine historical availability data and other pertinent metrics.

Our monitoring platform goes beyond traditional network managed service capabilities, providing advanced intelligence and proactive oversight to ensure optimal performance. Endpoint monitoring is conducted through protocols such as SNMP, WMI, API, and ICMP, it includes comprehensive hardware health monitoring, continuously assessing critical components such as CPU, memory, disk usage, and even power supplies for potential issues. The platform also utilises AI-driven learning to establish baselines of normal behaviour, enabling it to detect and respond to uncharacteristic patterns or anomalies proactively. When issues are identified an automatic fault is generated and escalated to the Principle Networks Service Desk for resolution. This proactive and intelligent approach ensures issues are addressed promptly, in line with the agreed Service Level Agreement (SLA), minimising downtime and enhancing overall reliability.

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 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 solutions.

Patch Management (High/Critical Vulnerabilities)

Principle Networks' Servicedesk team is responsible for applying patches to operating systems exposed to a critical or high-risk vulnerability. This task is performed proactively for supported vendors in accordance with our change management procedures during standard working hours. Out of hours patching can also be arranged without charge. We aim to complete these updates within 14 days of notification from the vendor in question.

Our proactive approach to patch management ensures the ongoing security and stability of your infrastructure. We are dedicated to protecting all managed devices from potential threats.

A patch is considered critical or High risk based on vendor CVE score, where Principle Networks confirmed the vulnerability impacts the service's functionality or security such as whether the impacted application is in use and exposed in the manner described by the vendor.

Patch Management (Non High/Non Critical Vulnerabilities)

For patches deemed non-critical or not high-risk, the standard change management process applies, and can either be explicitly defined as part of a server support model for OS patching or accounted for against a customer's pre-paid days contract where one exists.

Certificate Management

We take a proactive approach to certificate management. Our robust system monitors certificate expiration dates diligently. As soon as a certificate approaches 30 days of its expiry date, our ITSM will automatically raise a Change Request. We promptly notify our managed services customers, ensuring they have ample time to renew certificates before any potential service disruptions occur. With our expert's support to help replace expiring certificates and ensuring the solution remains secure and operational.

Certificate Management is limited to certain device types. We regularly add support for new device types and may add support for additional device types upon request where possible.

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. Generally, we expect customers to have access to their own environments (for example Microsoft Azure, AWS).

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 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 technology 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 will affect the managed service solution 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 prepaid days contract.

Vulnerability Scans of Internet Facing Virtual Appliances

Principle Networks conducts regular Vulnerability Scans on all managed internet facing virtual appliances to ensure that common ports are not left open, either by vulnerabilities or administrative error. By identifying and addressing potential vulnerabilities, we proactively enhance the security posture of our customer environments, safeguarding against threats and unauthorised access.

Azure Health

Principle Networks provides personalised best practices to optimise your Azure cloud deployments. Our focus is on helping you reduce costs, enhance security, improve reliability, and achieve operational excellence while tailoring our services to your specific needs. These practises include:

Cost Management

Principle Networks offer actionable insights and strategies to help you minimise cloud expenses without compromising performance or scalability:

- Identifying Idle Resources: Detect and address underutilised resources like virtual machines, storage, or databases, allowing you to shut down or resize them to cut unnecessary costs.
- Right-Sizing Resources: Analyse your usage patterns and recommend resizing or consolidating resources to meet your workload requirements efficiently.
- Purchasing Reserved Instances: Identify workloads suited for reserved instances, providing substantial savings compared to pay-as-you-go models.
- Cost Management Reports: Deliver in-depth reports on spending trends, highlighting actionable insights and an overall cost score to help optimise your budget.

By leveraging these cost-saving strategies, you can significantly reduce expenses and pay only for the resources you truly need.

Security

Principle Networks security services ensure your Azure environment remains protected, compliant, and resilient:

- Focus on critical and high-severity issues, with recommendations for medium/low severities as needed.
- Strengthen access management through measures like Multi-Factor Authentication (MFA) and enhanced account monitoring.
- Continuous compliance checks to ensure your resources align with Azure's best practices and regulatory standards.

A secure Azure environment that mitigates risks and provides peace of mind.

Reliability

We prioritise the resilience and availability of your Azure resources:

- Continuous monitoring of Azure health to identify and resolve potential issues proactively.
- Ensure redundancy and high availability for critical workloads.
- Focus on critical and high-severity impacts, providing tailored advice for medium/low severities.

A reliable Azure environment with minimal downtime and optimal resource availability.

Operational Excellence

Enhance your cloud operations by ensuring your environment runs efficiently and seamlessly:

- Identify and address dissociated or misconfigured resources that could impact performance.
- Minimise service desk tickets by implementing preventive measures and operational best practices.
- Focus on critical and high-severity issues, with advisories for medium/low severities to maintain operational standards.

A streamlined environment with reduced administrative overhead and improved end-user satisfaction.

Note: We prioritise addressing critical and high-impact severity issues, ensuring the most significant risks and challenges are resolved effectively. Medium and low-severity issues are monitored, with tailored recommendations provided as needed to maintain overall system health and performance.

Enhanced Cloud Managed Service Overview

Azure Site Recovery

Azure Site Recovery is a cloud-based disaster recovery service designed to maintain business continuity during planned and unplanned outages. It automates the replication of physical and virtual machines to Azure or a secondary location, enabling swift failover and recovery to meet specific Recovery Time Objectives (RTO). With support for both Windows and Linux systems, as well as integration with VMware and Hyper-V, Azure Site Recovery minimises downtime and data loss, ensuring robust disaster recovery.

The service also simplifies disaster recovery management by allowing you to orchestrate failover and recovery processes through a centralised Azure portal. Additionally, it includes disaster recovery testing capabilities, enabling you to test your recovery plans without disrupting live environments so you can ensure that your systems are always prepared for an emergency.

Backup / Configuration management

Azure Backup Service provides a secure, reliable, and scalable cloud-based backup solution for data protection. Utilising snapshot technology, it enables quick and efficient backups of virtual machines, databases, and files, which can be easily restored as needed. Much like VMware snapshots, Azure Backup ensures rapid recovery options to minimise downtime, all while adhering to industry best practices for data security and compliance.

For configuration backups, application features such as configuration difference comparisons can be used to checked for changes within a troubleshooting scenario, or they can be called upon for compliance purposes should this be necessary.

Recovery Point Objectives (RPO)

Recovery point objective or RPO is defined as the maximum amount of data measured in time that can be tolerably lost after a recovery from a disaster or failure.

Principle Networks fully understands the critically of data stored within the environment. The solution is built with Data Protection in-mind, with a combination of Local and Zone Redundant Storage (LRS, ZRS) for all non-temporary data disks within Azure Virtual Machines.
The following table described the Recovery Point Objective (RPO) for all Virtual Machines within the Azure hosted Environment.

Azure Hosted Environment – Backup Policy	
Hourly Backup Frequency	4 hours
Daily Backup Frequency	Every day
Retention of Daily Backups	180 days
Instant Restore from Snapshot	7 days

Example of a best practice Backup policy.

Business Continuity & DR Testing

Principle Networks offer comprehensive tools and services to ensure business continuity and effective disaster recovery (DR) testing. Key features include:

- **Automated Backups -** Securely automate backups of critical data and applications, ensuring quick recovery and minimal data loss.
- **Georedundant Storage -** Utilise geographically dispersed storage to protect against regional outages and ensure high availability.
- **Disaster Recovery Orchestration:** Implement automated DR plans with predefined failover and failback processes, reducing manual intervention during emergencies.
- **Scalable DR Infrastructure -** Scale DR resources on-demand to meet your business needs without the high costs of traditional DR setups.
- **Regular DR Drills -** Conduct regular, non-intrusive disaster recovery drills to validate and improve your recovery plans.
- **Compliance and Auditing -** Maintain detailed logs and reports to ensure compliance with industry standards and facilitate audits.

Using cloud solutions for BCDR testing ensures that your business remains resilient, data stays secure, and operations can quickly resume after a disruption.

Microsoft Entra ID Identity & Access Management

Identity & Access Management (IAM) offers comprehensive solutions to safeguard your organisation's resources while enhancing operational efficiency. Key features include:

- **Active Directory (e.g. Azure AD / Entra) -** Centralised identity management with single sign-on (SSO), multi-factor authentication (MFA), and conditional access policies.
- **Role-Based Access Control (RBAC) -** Fine-grained access control to resources, ensuring users have only the permissions they need.
- **Identity Protection -** Advanced threat detection and mitigation for identity-based attacks.
- **Self-Service Capabilities -** Empower users with self-service password reset and group management, reducing IT support overhead.
- **Integration –** Supporting organisational security objectives and reducing administrative overhead by scoping, delivery and support a wide range of 3rd party IdP integrations utilising industry standard protocols such as SAML2.0 and Oauth2 to ensure 3rd party applications adhere to corporate policy and user/identity management.
- **Compliance and Auditing -** Detailed logging and reporting to meet regulatory compliance and audit requirements.
- **Identity Risk –** Proactively monitor device and user risk against normal identity behaviours and respond automatically where risk are identified, such as where a user is attempting to access key systems from multiple locations or from a untrustworthy location, at a unusual time, or through a method that is out of character.

Utilising IAM, you can enhance security, simplify access management, and ensure compliance, all while providing a seamless user experience across your organization.

Microsoft Intune Mobile Device Management (MDM)

Microsoft Intune, or Endpoint Manager is Microsoft SaaS based Mobile Device Management (MDM) software. Intune is the central control point for configuring, managing and automatic deployment of devices, policies and applications to Endpoints, including Windows computers, Android and iPhone devices.

Microsoft Intune is also included in Microsoft365 E3 licenses (and others) and enables fully automated self-service deployment of corporate Windows devices, as well as corporate and 'Bring your own device' (BYOD) mobile phones.

As the central control point Intune is where most of an organisations MDM configuration will reside to ensure that the organisation can automate the deployment of corporate windows devices using Microsoft Autopilot and well as policies and day to day administrative tasks assigning new applications to end users.

Principle Networks offers end to end solution to scope, deliver and support Intune deployments, including but not limited to zero touch autopilot deployment of Windows devices, Microsoft Defender integration and best practice configuration and security policies and application deployment and management.

Note: Autopilot deployment must be specified when order Microsoft devices from the customer's chosen supplier in order to support zero touch self-service deployment for users.

Platform Automation and DevOps

Cloud solutions for Platform Automation and DevOps enable efficient development, deployment, and management of applications. Key features include:

- **Continuous Integration/Continuous Deployment (CI/CD) -** Automate build, test, and deployment processes, ensuring rapid and reliable delivery of code changes.
- **Infrastructure as Code (IaC) -** Manage and provision infrastructure using code enabling consistent and repeatable setups.
- **Automated Scaling -** Dynamically adjust resources based on demand, ensuring optimal performance and cost-efficiency.
- **Monitoring and Logging -** Utilise integrated monitoring and logging tools for real-time insights, proactive issue detection, and swift resolution.
- **Collaboration Tools -** Enhance team collaboration with integrated project management, version control, and communication tools.

By leveraging cloud-based Platform Automation and DevOps, you can accelerate development cycles, enhance reliability, and foster seamless collaboration across your teams.

External Vulnerability Testing

External vulnerability testing is a key component of maintaining a secure IT environment. Here is a more detailed explanation of the process and its benefits:

Vulnerability testing, also known as vulnerability assessment, is the process of identifying, classifying, and prioritizing vulnerabilities in computer systems, applications, and solution infrastructures. It provides organizations with the necessary information to understand and mitigate risks associated with these vulnerabilities.

Detailed Reports - After conducting vulnerability tests, detailed reports are generated. These reports typically include:

- **Risk Levels** - Each vulnerability is categorized by its risk level, from critical to low.
- **Vulnerability Details** - Information about the nature of each vulnerability, how it can be exploited, and the potential impact.
- **Remediation Steps** - Recommended actions to fix or mitigate the vulnerabilities.
- **Compliance Status** - Assessment of how the vulnerabilities affect compliance with relevant regulations and standards.

Benefits of Regular Testing:

- **Proactive Security** - Regular testing helps in identifying vulnerabilities before they can be exploited by attackers.
- **Risk Management** - By understanding the risk levels, organizations can prioritize their response efforts effectively.
- **Compliance Assurance** - Regular assessments ensure that systems remain compliant with industry standards and regulations.
- **Trust and Reliability** - It builds trust with customers and partners by demonstrating a commitment to security.

External vulnerability testing provides detailed reporting and is essential for any organization looking to secure its IT services and protect against emerging threats. It is a proactive measure that not only enhances security but also supports compliance and operational reliability.

Business Review

Business Reviews comprises of a Service Management Review, Security Review, Technology Review and a Business Update and can be added to the service, typically on a quarterly basis.

During the Business Review, we present a PowerPoint Presentation prepared during the initial phase. The appropriate parties (Service Manager, Solutions Architect, Account Manager, etc.) leads the discussion, with the final stage facilitated by the Account Manager.

Service Management Review

- The Service Manager provides an in-depth analysis of service levels, cases, and overall performance.
- We discuss how well Principle Networks met Service Level Agreement (SLA) Key Performance Indicators (KPIs).
- Challenges related to service delivery within the customer's business context are addressed.

Security Review

- This section focuses on security services purchased through Principle Networks (e.g., external penetration testing, Firewalls, Zscaler, Microsoft IAM, Cisco Umbrella etc.).
- We review findings since the last Business Review, including documented security events and attacks.
- High-risk events or security cases are discussed.
- Both the Service Manager and Cyber Security Consultant (or Solution Architect) contribute to this section.

Technology Review

- The Solution Architect or Subject Matter Expert (SME) leads the Technology Review.
- Opportunities for new solutions, licensing, and existing technology deployments are highlighted.
- Customer interests and follow-up actions are recorded.

Business Update

- The Account Manager manages the final stage of the Business Review.
- We invite the customer to discuss their business plans, key strategic objectives, and any relevant changes or developments so Principle Networks can better align our service to support the customer.

Overall, the business review meeting is designed to ensure that all aspects of the company's operations are aligned with strategic goals, risks are managed effectively, and opportunities for growth and improvement are identified and acted upon.

For more information or to schedule a Business Review, please feel free to reach out to your account or service manager. We value our partnership and look forward to continued collaboration.

Cloud Firewall Review

Principle networks offers a comprehensive Firewall Review the process involves the following steps and is not limited to (Example based around an Azure Firewall or other NVA such as a virtual Fortigate):

Current Firmware Assessment

- Our team begins by assessing the current firmware version of your firewall.
- We gather information about the existing setup, including specifications.

Upgrade Options Evaluation

- We explore upgrade options available for your firewall.
- This includes researching the latest firmware releases and compatibility with your specific model.

Release Notes Examination

- Our experts meticulously review the release notes provided by the firewall vendor.
- We pay attention to new features, bug fixes, and security enhancements.

Special Notices and Known Issues

- We identify any special notices or known issues associated with the proposed firmware upgrade.
- Transparency is crucial—we communicate any potential impact on your network.

Support Assessment

- As part of the process, we evaluate support.
- If any components require replacement or if technical assistance is needed (TAC), we address it proactively.

Additional Security Features

- Review of current licensing and features.
- Assess possible security enhancements based on unutilised capabilities.
- Technical guidance of implementation of features.

Risk Identification

- We assess the risks associated with the upgrade.
- Factors such as downtime, compatibility, and potential disruptions are considered.

Pre-Upgrade Checks

- Before proceeding, we perform thorough pre-upgrade checks.
- This ensures that the network environment is ready for the firmware update.

Upgrade Execution

- Our team executes the firmware upgrade following best practices.
- We minimize downtime and closely monitor the process.

Post-Upgrade Validation

- After the upgrade, we validate the firewall’s functionality.
- We ensure that all services are operational and security settings remain intact.

User Acceptance Testing (UAT)

- We collaborate with your team to create a UAT test plan.
- This involves testing critical functionalities and verifying that the firewall meets your requirements.

Documentation and Communication

- We document the entire process, including upgrade details and any adjustments made.
- Clear communication ensures that your team is informed about the changes.

At Principle Networks, we prioritise security, reliability, and seamless transitions. If you have any questions or need further assistance, feel free to reach out.

Appendix

Minimum Data Set (Incident Ticket)

It is the responsibility of the customer to provide as much information about an incident as possible to enable Principle Networks to respond efficiently and resolve the issue as quickly as possible. Here is a guide to help provide a minimum set of information to the Servicedesk upon logging a case.

- Date and time problem occurred:
- Detailed Description of the fault/change request:
- Asset(s) affected if known:
- Any recent changes made:
- What is the impact to the customers business (often dictates the priority):
    - No. Sites affected:
    - No. Users Affected:
- Specific error messages (if applicable):
- Screenshots attached? Yes/No:
- Troubleshooting steps tried to resolve the issue so far?:

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	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 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	Senior Servicedesk Engineer	0333 012 4003	servicedesk@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 service 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.

Principle
networks

Technology
Delivered
Better

03330 124 003
enquiries@principle-networks.com
www.principle-networks.com