Effective January 05, 2026. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

MANAGED SERVICES

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

ManageIT Products

Helpdesk Support

ManageIT CORE Services

Help Desk Access (Email, Chat & Portal)

Support includes assistance on devices and software that meet support eligibility in areas like Office applications, email access, internet connectivity, printers, and basic device troubleshooting.

ManageIT PLUS Services

Help Desk Voice and Phone Support

Technicians provide guidance and remote device support for resolving issues that require live interaction.

User Device Setup

Support provides remote assistance to help users log into their domain and access their applications and data. Technicians guide users through the login process, verify access, and ensure they can reach the resources assigned to them.

Mobile Phone Support

Support is provided remotely for mobile devices that meet support eligibility. Technicians walk users through the steps needed to access email, calendar services, business applications, and other

assigned resources, assist with basic device troubleshooting, and provide help with Mobile Device Management enrollment and remote wipe requests.

Inactive User Reporting (RITIS)

Our Realtime Intelligence Technology Information System (RITIS) provides automated reporting that identifies dormant user accounts in your environment. The system automatically detects user accounts without recent activity based on configurable inactivity thresholds aligned with your organizational policy. Dashboard visibility provides insight into inactive account status, helping identify license reclamation opportunities and potential security risks from orphaned accounts.

Inactive User Reviews & Recommendations

DivergeIT conducts periodic analyses of inactive user accounts with actionable recommendations for account lifecycle management. Detailed reports categorize recommendations for accounts that should be disabled, archived, or deleted. Review meetings are available upon request to discuss license optimization suggestions and security risk assessments for orphaned accounts that may pose compliance or security concerns.

Inactive User Auto-Disabling

Automated account disabling reduces security exposure by disabling accounts after a configurable inactivity period. The system sends automated pre-disablement notifications to users and their managers before taking action, maintaining a complete audit trail of all automated account actions. An exception process accommodates accounts requiring extended inactivity periods. Reactivation of disabled accounts is handled via standard support tickets subject to standard SLAs.

Server Support & Management

ManageIT CORE Services

Server Support & Troubleshooting

Remote support is provided for servers that meet support eligibility. Technicians troubleshoot issues, perform root cause analysis for recurring problems, and coordinate with hardware vendors for warranty support. Physical hardware failures requiring on-site intervention are coordinated with your designated on-site contact or hardware vendor. On-site technician dispatch is not included.

Patch & Update Management

Security patches and updates are applied to eligible servers using a phased ring deployment strategy to minimize risk. Technicians perform routine patch assessments and deployments to maintain security and stability.

Monitoring & Logging

Automated 24/7 monitoring tracks critical health metrics on eligible servers, including CPU, memory, disk, and network utilization. Alerts based on configurable thresholds notify technicians of potential issues, and event correlation enables proactive problem identification. Centralized log collection with 7-day rolling retention supports rapid troubleshooting and audit compliance. Long-term log archival for compliance requirements is available with SecureIT Max.

User & Group Management

Standard Move/Add/Change requests are administered for user accounts, security groups, and access permissions on eligible servers. This includes Active Directory user and group administration and Group Policy enforcement. Structural Active Directory changes, domain migrations, and full security permission audits are classified as Projects and not included.

Server Performance Incident Reporting

When performance incidents occur on eligible servers, technicians provide documentation including a detailed timeline, impact assessment, and root cause analysis to identify recurring issues. Deep-dive forensic analysis, application code debugging, and data recovery services are not included.

Cloud Support & Troubleshooting

Remote support is provided for eligible cloud-hosted server infrastructure, including troubleshooting of cloud resource issues, root cause analysis for service disruptions, coordination with cloud provider support, and emergency response for critical outages. Support is limited to operating system and cloud resource configuration layers. DivergeIT manages the tenant and subscription but does not guarantee the availability or SLA of the underlying cloud service provider infrastructure, such as GCP or Azure outages.

Cloud Spending Insights Report

Periodic cost analysis is provided for eligible cloud resources, including detailed breakdown by resource type, cost trending and forecasting, comparison to budget and prior periods, and actionable cost reduction recommendations. Technical execution of cost-saving changes, such as re-architecting applications to use cheaper storage tiers, is classified as a Project and not included.

Resource Inventory Reporting

Comprehensive inventory of all cloud resources includes complete resource enumeration across subscriptions, configuration and sizing documentation, tagging compliance reporting, and resource relationship mapping. This visibility is essential for cost management, security, and compliance.

ManageIT PLUS Services

Storage Management

Storage management for eligible servers includes disk space monitoring and alerting, storage cleanup recommendations, cloud storage integration support, and external storage configuration. Cleanup services are limited to temporary system files and caches. Organization or deletion of user-generated content such as documents and photos is the user's responsibility. Mass data migration to cloud storage is classified as a Billable Project and not included.

Network Configuration Management

Network settings and connectivity are managed for eligible servers, including IP address and DNS configuration, network interface and NIC teaming configuration, and local firewall rule management. Physical network infrastructure such as cabling and switches, and ISP-related troubleshooting, are not included unless a Network Support plan is active.

Server Performance Monitoring & Optimization

Proactive performance management is provided for eligible servers, including CPU, memory, and disk performance analysis, baseline establishment, and configuration optimization recommendations. Optimization is limited to OS and resource allocation settings. Application code refactoring and database query tuning are not included.

Application & Service Maintenance

Technicians maintain the availability of eligible Windows services and agreed-upon line-of-business applications. This includes service monitoring, restarting hung services, and troubleshooting connectivity. Major version upgrades, new application deployments, database administration, and architectural changes are classified as Projects and not included.

Virtualization Maintenance

Technicians maintain the health of eligible host and guest operating systems in virtualized environments. This includes resource allocation adjustments and snapshot management. Building new VM farms, host migrations, and physical-to-virtual server conversions are classified as Billable Projects and not included.

Remote Access & Management

Secure remote access to eligible servers is configured and managed, including Remote Desktop Services configuration and VPN management. Management is limited to access infrastructure only. The client is responsible for managing third-party vendor access and ensuring vendor compliance with security policies.

Web Application Single Sign-On

SSO integrations are managed for eligible web-based applications, including SSO configuration, federation trust management, and certificate management. Support is limited to standard SAML/OIDC configurations with Microsoft Entra ID and Google Workspace. Adding additional applications and custom API development or integration with non-standard applications are classified as Billable Projects and not included.

Server Downtime Incident Reports

When outages occur on eligible servers, technicians provide documentation including detailed incident timelines, business impact assessment, and root cause analysis. Root cause analysis is limited to operating system and infrastructure logs. If the root cause is determined to be a third-party application bug, the analysis will conclude with that finding.

CPU/Memory/Disk Usage Monitoring & Alerts

Real-time monitoring of resource utilization is provided for eligible servers, including configurable threshold-based alerting and proactive capacity exhaustion warnings. Technicians provide alerts and capacity recommendations. Remediation requiring disk space expansion, hardware procurement, or migration of data to new volumes is classified as a Billable Project and not included.

ManageIT PRO Services

High Availability & Failover

Existing clustering and failover configurations are managed for eligible business-critical systems, including health monitoring of replication status and cluster nodes. Support is limited to Windows Server and Microsoft SQL clustering. Failover testing, disaster recovery drills, and build-out of new high-availability clusters are classified as Billable Projects and not included.

Server Uptime Monitoring & Dashboards

Customizable dashboards provide visibility into availability metrics for eligible servers, including real-time uptime and downtime tracking. Uptime reporting reflects operating system availability. Outages caused by ISP failures, power loss, or third-party application crashes are annotated as exceptions to infrastructure uptime SLAs.

Budget Alerts & Resource Tagging

Cost management controls are provided for eligible cloud resources, including budget threshold alerting configuration, resource tagging strategy implementation, tag compliance monitoring and remediation, and cost allocation by tag, project, or department. Tagging policies are enforced for newly created resources. Retroactive manual tagging of existing or historical resources is classified as a Billable Project and not included.

Orphaned Resource Discovery & Remediation

Unused cloud resources are identified to help optimize spending on eligible cloud environments, including automated detection of unattached disks, IPs, and snapshots. Monthly reporting and cleanup tasks are provided for resources generated during the active contract term. Remediation of historical technical debt or bulk cleanup of resources pre-dating the agreement is classified as an Onboarding Project and not included.

Cost Optimization Recommendations & Auto-scaling

Proactive cost management is provided for eligible cloud resources, including right-sizing recommendations based on utilization, reserved instance optimization, auto-scaling policy configuration and tuning, and identification of spot or preemptible instance opportunities. Designing and implementing new auto-scaling architectures, such as refactoring monolithic applications for scale sets or spot instances, is classified as a Billable Project and not included.

Workload Optimization & Right-sizing

Workload analysis is provided for eligible cloud resources, including VM size optimization recommendations, storage tier optimization, and migration path recommendations. Execution of resizing tasks that require maintenance windows or downtime is coordinated as a standard Change Request.

AugmentIT Optional Services

Onsite Server Support

Onsite Server Support provides scheduled in person assistance for server issues that require a

technician to be physically present. Technicians can perform onsite checks, assist with hardware related tasks, and work with onsite contacts to help restore normal server operation.

Advanced Patch Validation

This service provides custom pre-deployment testing of updates in a dedicated lab environment before they are released to production systems. Technicians validate update behavior, identify potential issues, and review compatibility with supported applications. If a deployed update causes problems, technicians perform best effort rollback to restore normal operation.

Computer Support & Management

ManageIT CORE Services

Support & Troubleshooting

Remote assistance is provided for computers and laptops that meet support eligibility. Technicians help users troubleshoot issues, diagnose problems, and access their applications and services. Support includes help with Microsoft 365, Office applications, email access, internet connectivity, printers, and basic device functionality. Technicians guide users through the steps needed to resolve issues and can remotely access the system when necessary to restore normal operation.

Monitoring & Logging

Remote monitoring identifies issues through alerts generated by the **provided** RMM agent. Technicians review these alerts, respond as needed, and take action to help maintain system performance and reliability.

User Account Creation & Management

Local and domain user account administration includes local user account creation, domain join, and profile setup. Note: Service covers standard user provisioning based on existing templates. Complex "white glove" onboarding setups exceeding 60 minutes per user are classified as Billable Projects.

Patch & Update Management

Security patches and updates are applied to eligible servers using a phased ring deployment strategy to minimize risk. Technicians perform routine patch assessments and deployments to maintain security and stability.

Password Management

This service includes assistance with password related access issues such as password reset support, self service reset enablement, and Keychain assistance for macOS. Technicians maintain passwords specific to eligible devices that are managed, but user passwords are not stored. Password resets require user validation using approved verification tools or approval from a designated point of contact.

Access Control & Permissions Management

This service includes maintaining and repairing file, folder, and application access permissions, including adjustments to existing permission structures and administrative rights. New permission design or restructuring is not included. All access change requests require approval through the ticket approval system.

Hardware Failure Incident Reports

When hardware issues are detected, technicians provide incident documentation that includes failure diagnosis, warranty status verification, and coordination of warranty claims when applicable.

ManageIT PLUS Services

Software & Application Management

Application management includes installation and configuration of eligible software, assistance with application updates, and support for accessing business productivity tools such as Office, browsers, and communication applications. Technicians help ensure applications are available, properly configured, and functioning so users can access the tools they need.

Lifecycle Management

Device Lifecycle Management includes tracking device age and warranty status, planning refresh cycles, providing replacement recommendations, and performing technology currency assessments. Technicians help ensure users have reliable and secure devices through proactive lifecycle oversight.

Asset Lifecycle Tracking & Refresh Planning

Strategic planning for device refresh includes asset inventory maintenance, refresh schedule development, budget planning support for hardware refresh, and procurement specification recommendations. Planning ahead enables budget predictability and ensures timely device replacement.

ManageIT PRO Services

Storage Management

Local storage management includes disk space monitoring through the provided RMM, alerting, cleanup recommendations, cloud storage integration assistance, and support for configuring external storage on eligible devices. Technicians help users maintain available disk space and prevent interruptions caused by storage limitations.

Profile and Data Management

Profile and Data Management includes configuring and troubleshooting user profiles, assisting with data access, and helping users maintain access to their settings, applications, and stored data on eligible devices. Data recovery is provided when the user is covered by a backup eligible product.

AugmentIT Optional Services

Forensic Data Recovery Services

Forensic Data Recovery Services provide specialized retrieval of data from physically damaged or inaccessible storage devices. This process uses advanced diagnostic tools, clean room techniques, and specialized equipment to recover data from drives affected by mechanical failure, electrical damage, corruption, or other forms of physical impact.

Advanced Patch Validation

This service provides custom pre-deployment testing of updates in a dedicated lab environment before they are released to production systems. Technicians validate update behavior, identify potential issues, and review compatibility with supported applications. If a deployed update causes problems, technicians perform best effort rollback to restore normal operation.

Device Disposition and Data Sanitization

Device Disposition and Data Sanitization **include** coordinating end of life device handling and performing remote data sanitization when possible. Technicians guide clients through proper device disposition procedures to support secure retirement of hardware.

Printer Management Services

ManageIT CORE Services

Printer Support & Troubleshooting

Support includes troubleshooting print jobs, resolving connectivity problems, installing and updating drivers, and managing print queues for eligible printers and devices. Technicians provide remote assistance to walk users through addressing basic hardware related issues such as power interruptions and simple device checks and help ensure printers remain accessible on the network.

ManageIT PLUS Services

Printer Management

Printer Management includes monitoring network printer availability, identifying issues that may affect printing, managing firmware updates, and supporting connectivity for eligible printers and devices. Technicians address printing problems such as queue issues, connectivity, and accessibility, and provide remote assistance to help ensure printers remain available on the network.

ManageIT PRO Services

Printer Setup & Configuration

Printer Setup and Configuration includes deploying network printers, configuring print settings, and assisting users with connecting to shared printers on eligible devices. A ticket support template must be completed by the vendor or the customer to ensure all required information is provided for proper setup. Technicians help ensure printers are configured correctly and accessible so users can begin printing successfully.

Network Support

ManageIT CORE Services

DNS Support & Troubleshooting

Support includes assisting with DNS resolution issues, verifying record propagation, and helping configure DNS settings for services such as mail authentication on eligible systems. Technicians review DNS records, identify issues that may affect service availability, and provide guidance to ensure reliable name resolution and service connectivity.

ManageIT PLUS Services

Switch Support - Network Monitoring

Network Support includes remote monitoring of network switch health and performance on eligible devices, including switch status, port activity, and uptime. Technicians review alerts, respond to issues, and provide remote assistance to help maintain a stable and reliable network environment.

Switch Troubleshooting & Diagnostics

Troubleshooting and Diagnostics includes remote assistance for identifying and resolving issues within the network infrastructure on eligible devices. Technicians help diagnose connectivity problems, review switch activity, and guide users or onsite staff through steps needed to restore normal network operation.

Switch Documentation & Inventory Management

This service includes maintaining up to date documentation for eligible network devices, including topology details, switch configuration backups, and current equipment listings. Technicians ensure documentation reflects changes made during support activities, so the environment remains accurate and easy to troubleshoot.

DNS Monitoring & Reporting

Monitoring and Reporting includes continuous monitoring of DNS availability and query response performance on eligible systems. Technicians review alerts and performance data to help identify and address DNS issues before they impact users.

DNS Configuration Management

DNS Configuration Management includes creating and updating DNS records and managing zone configurations for standard record types such as A, CNAME, MX, TXT, and others. Technicians help ensure DNS entries remain accurate and support reliable service connectivity.

SSL Certificate Management

This service includes monitoring SSL and TLS certificate expiration, providing alerts, coordinating renewals, and assisting with certificate installation on eligible systems.

Firewall & WAN Availability Monitoring

This service includes continuous remote monitoring of firewall and WAN availability on eligible devices, providing visibility into uptime and link status. Technicians review alerts, respond to detected issues, coordinate with the ISP when connectivity problems are identified, and provide remote support to bring the firewall back online when necessary.

Firewall Configuration Support

This service includes assistance with creating and modifying firewall rules, updating policies, and configuring NAT or port forwarding on eligible devices. Technicians help ensure firewall settings support secure and reliable access for users and systems.

WAN VPN Management

This service includes configuring and maintaining site to site VPN connections and assisting users with remote access VPN connectivity on eligible devices. Technicians help ensure the VPN gateway and client software are properly configured, guide users through connection steps, and provide remote support to help restore access when issues arise.

Firewall Decryption & Inspection Management

This service includes maintaining SSL and TLS decryption policies, managing certificates required for inspection, and supporting ongoing traffic inspection on eligible devices. Technicians help ensure decryption and inspection configurations remain stable and continue to operate as intended.

Firewall Access & Control Management

This service manages all administrative access to eligible firewall systems. Technicians maintain administrator accounts, configure role based access controls, and manage multi factor authentication for administrative entry. When a firewall is under our management, we serve as the sole administrator to ensure consistent configuration control and prevent unauthorized changes.

Wireless Network Availability Monitoring

This service includes remote monitoring and support for wireless access points on eligible devices. Technicians monitor uptime, review signal strength indicators, respond to alerts, and provide remote assistance to help maintain stable wireless connectivity.

Network Wireless Support

This service includes remote assistance for wireless connectivity issues on eligible devices. Technicians help troubleshoot client connection problems, resolve authentication issues, and guide users through the steps needed to regain reliable wireless access.

Network Wireless Firmware & Software Update Support

This service includes monitoring firmware versions for wireless infrastructure on eligible devices, planning updates, and coordinating remote deployment. Technicians help ensure wireless systems remain current, stable, and supported through routine update management.

ManageIT PRO Services

Switch Advanced Monitoring & Performance Management

This service includes enhanced monitoring for eligible network devices, including bandwidth utilization visibility, Quality of Service configuration, and traffic pattern analysis. Technicians review performance data to help identify issues and maintain a reliable and responsive network experience.

Switch VLAN Management

VLAN Management includes creating and adjusting VLANs, assigning ports, and configuring inter VLAN routing on eligible network devices. Technicians assist with routine VLAN changes that support user and device connectivity.

Switch High Availability & Redundancy

This service includes maintaining and validating existing high availability and redundancy configurations on eligible network devices. Technicians assist with configuration checks, monitoring redundancy status, and supporting failover validation to help ensure continuity during device or link interruptions.

DNS Registrar Management

This service includes managing domain registrar accounts, assisting with domain lock and unlock actions, updating registration details, and configuring WHOIS privacy settings. Technicians act as the technical contact while ensuring the domain remains properly maintained.

DNS Domain Procurement

This service includes assisting with new domain registration, searching for available domain names, and completing initial DNS configuration to bring the domain online.

Advanced Monitoring & Logging

This service includes enhanced traffic and security event visibility on eligible devices. Technicians review logs, analyze traffic patterns, and respond to threat detection alerts to support timely incident investigation. Standard log retention of 30 days is included.

Network Firmware & Software Updates

This service includes monitoring firmware and software versions on eligible devices, planning updates, and coordinating change windows. Technicians perform remote updates to help keep systems current and stable.

Firewall NAT Management

This service includes configuring and maintaining static and dynamic NAT settings on eligible devices, including creating and updating port forwarding rules. Technicians help ensure NAT configurations support secure and reliable access for users and services.

Network Wireless Advanced Monitoring & Logging

This service includes enhanced wireless monitoring on eligible devices, providing visibility into client usage patterns, bandwidth consumption, and detection of unauthorized access points. Technicians review monitoring data and alerts to help maintain a secure and reliable wireless environment.

AugmentIT Optional Services

Network Physical Layer Support

This service provides onsite assistance for troubleshooting and resolving issues that require hands on work. Technicians can perform tasks such as cable tracing, testing wall jacks, validating network runs, assisting with hardware placement, and coordinating with onsite staff to confirm physical connectivity. The service also includes support with ISP related issues by assisting with onsite verification steps, gathering required information, and coordinating updates with the provider to help restore service.

Onsite Wireless Mapping and Analysis

This service provides onsite evaluation of wireless coverage and performance. Technicians perform physical site surveys, heat mapping, and identify coverage gaps or signal issues. This service can also include physical relocation of access points when cabling work is required, ensuring the wireless layout supports reliable connectivity throughout the environment.

Advanced Wireless Diagnostics

This service includes advanced troubleshooting and performance analysis for wireless environments on eligible systems. Technicians analyze wireless performance data, review signal behavior, evaluate channel usage, and identify factors affecting coverage or connectivity to support improved wireless performance.

Switch Network Segmentation

Network Segmentation Projects cover large scale tasks such as designing new VLAN structures, re IP planning, and implementing segmentation changes across the entire environment.

Switch High Availability Architecture and Implementation

This service covers the design and implementation of new high availability and redundancy architectures. Technicians plan and configure systems such as gateway redundancy, link redundancy, and failover paths to enhance network resilience and support business continuity requirements.

DNS Advanced Traffic Management

This service includes designing and configuring enhanced DNS features such as geographic based routing, weighted load distribution, failover routing policies, and other advanced traffic control methods. Technicians implement traffic strategies that improve availability, performance, and resilience across distributed environments.

SSL Certificate Acquisition

This service includes assisting with obtaining SSL and TLS certificates, gathering required information, preparing certificate requests, and coordinating delivery of the certificate to the client or hosting provider.

SSL Application Configuration Changes

This service includes making application related configuration updates needed to support SSL and TLS usage, such as updating application settings, adjusting redirect rules, and confirming the application is responding correctly after certificate changes.

Domain Negotiation Services

This service includes assisting with the negotiation and acquisition of squatted, premium, or aftermarket domains. Technicians help evaluate domain options, coordinate communication with sellers or brokers, and support the client throughout the negotiation process.

Firewall Advanced Architecture Changes

This service includes designing and implementing complex firewall architecture updates on eligible devices, including multi zone designs, advanced security policies, high availability configurations, and changes that require coordinated maintenance windows. Technicians plan and apply architectural updates to enhance security, performance, and resilience.

Firewall Decryption and Inspection Implementation

This service includes designing and implementing SSL and TLS decryption and deep packet inspection on eligible devices. Technicians configure required policies, certificates, and inspection settings to establish new decryption capabilities and support secure traffic analysis.

Advanced Monitoring and Logging Extended

This service expands monitoring and logging capabilities on eligible devices to include extended log retention beyond 30 days, deeper event analysis, and enhanced reporting. Technicians maintain long term visibility into security and performance events to support audit, compliance, and extended investigative needs.

Onsite Network Firmware Remediation

This service provides onsite assistance when a firmware or software update on an eligible device requires physical intervention. Technicians perform onsite checks, connect to the device through console access when needed, and assist with recovery steps to help restore the device to operational status.

Advanced NAT Architecture

This service includes designing and implementing advanced NAT and network segmentation architectures on eligible devices, such as complex DMZ layouts, multi zone NAT structures, and specialized translation requirements. Technicians plan and apply architectural configurations to support enhanced security and application accessibility.

Immutable Backup Support & Management

ManageIT CORE Services

Cloud Workspace Backup (M365 & Google) This service includes the management of cloud-to-cloud backups for Microsoft 365 and Google Workspace environments. Technicians monitor the protection of emails, calendars, contacts, and file storage (OneDrive, SharePoint, Google Drive) to ensure data is recoverable. Support includes granular restoration of lost or deleted items to protect against accidental deletion or malicious activity.

ManageIT PRO Services

Monitoring & Reporting

This service includes continuous monitoring of immutable backup jobs on eligible systems, including confirmation of successful backups, visibility into failures, and tracking of storage capacity. Technicians review backup alerts and provide reporting to help ensure backups are completed as expected.

Incident Response & Troubleshooting

This service includes investigation of backup issues, analysis of failures, troubleshooting of backup agents, and assistance with granular data recovery such as individual files, folders, and virtual machines. Technicians provide support for backup operations and assist users in accessing recoverable data based on the capabilities of the system.

Failed Recovery Test Reports

Documentation of recovery test outcomes includes test result documentation and root cause analysis for failures identified during automated verification processes. This ensures visibility into the recoverability of the protected systems.

Backup Failure Incident Reports

Detailed documentation of backup failures includes a failure timeline and impact assessment. Incident reports are generated for critical or recurring failures to provide a clear record of resolution steps and system reliability.

Backup Storage Full Alerts

Proactive alerting for storage capacity includes utilization monitoring and capacity planning recommendations. Technicians identify when storage limits are approaching and provide recommendations to adjust retention or increase capacity.

Network Configuration Error Reporting

Detection of network issues affecting backups includes network connectivity monitoring for backup agents and bandwidth issue identification. Technicians diagnose the specific network blocks affecting the backup process to speed up resolution.

Network Outage Incident Reporting

Remote documentation of network outages impacting backups includes outage impact documentation, backup job correlation, recovery recommendations, and SLA tracking. Understanding outage impacts helps prioritize network stability improvements.

Automated Boot Verification

Automated recovery testing includes scheduled boot tests and screenshot verification of successful startups for eligible systems. This validates that systems can be recovered and booted effectively when needed.

Backup Success Rate Monitoring & Dashboards

Comprehensive remote dashboards provide visibility into success rate trending, job duration analysis, and data change rate monitoring. This data helps track the overall health and reliability of the backup environment over time.

Storage Capacity Monitoring & Retention Policy Review

Backup storage management includes utilization trending and retention policy compliance verification. Proper retention management ensures the organization balances data protection requirements with available storage resources.

Configuration Compliance Scanning

Verification of existing backup configurations includes policy compliance checking, configuration drift detection, remediation recommendations, and compliance reporting to ensure backup settings remain consistent with established standards.

Bandwidth Utilization Monitoring & Alerts

Remote monitoring of backup traffic includes bandwidth consumption tracking, peak usage identification, throttling recommendations, and schedule optimization suggestions to prevent backup jobs from impacting business network performance.

Storage Management

Storage administration includes storage allocation management, data deduplication monitoring, storage health monitoring, and expansion planning for existing storage environments.

ManageIT PLUS Services

RTO/RPO Analysis & Optimization

Analysis of recovery objectives includes current Recovery Time Objective (RTO) and Recovery Point Objective (RPO) assessment, gap analysis against business requirements, optimization recommendations, and architecture improvement suggestions.

Failure Pattern Analysis & Preemptive Adjustments

Proactive remote analysis includes historical failure review, pattern identification, and risk mitigation recommendations for existing configurations. Learning from past failures helps prevent future issues and improves overall backup reliability.

Scheduled Recovery Testing & Documentation

Regular recovery testing includes the documentation and review of automated quarterly test results, compliance sign-off, and continuous improvement tracking. This ensures adherence to established testing schedules and provides evidence of recoverability.

Data Verification & Testing

Backup data verification includes monitoring for application consistency (e.g., VSS writers), compliance verification, and automated integrity checks provided by the backup software to ensure the data within the backup is valid and usable.

AugmentIT Optional Services

Custom Backup Reporting

This service provides customized reporting for backup environments, including tailored summaries, trend analysis, capacity forecasting, and audit focused reporting based on client requirements. Technicians generate reports aligned to the client's preferred format, frequency, and data needs.

Disaster Recovery Execution

This service provides full scale disaster recovery assistance for rebuilding infrastructure following major events. Technicians coordinate system restoration, recover supported workloads, and assist in bringing critical services back online during large scale recovery efforts.

Backup Recovery Assistance (Customer Provided Solution)

This service provides recovery support for environments affected by basic data loss, widespread data loss or ransomware recovery when the backup system in use is not provided by DivergeIT. Technicians analyze the available backup media, assist with recovery options, and guide clients through restoration efforts using the third-party backup tools available in the environment.

Microsoft 365 User Support & Management

ManageIT CORE Services

User Management

This service includes remote administration for eligible Microsoft 365 user accounts, including account creation, license assignment, group management, and role delegation. Technicians handle routine moves, adds, and changes for existing workflows.

Service Health & Incident Management

This service includes monitoring Microsoft 365 service status for eligible tenants, communicating incidents to stakeholders, coordinating with Microsoft support, and assessing impact. Technicians help ensure visibility into platform health and support response efforts during service disruptions.

Email & Exchange Online Management

This service includes administration for eligible Exchange Online environments, including mailbox creation and management, shared mailbox configuration, mail flow rule management, and retention policy configuration. Technicians help ensure email services remain properly configured and operational.

SharePoint & OneDrive Management

This service includes administration for eligible SharePoint Online and OneDrive environments, including site collection management, permission configuration, storage quota management, and external sharing configuration. Technicians help ensure collaboration services are properly maintained.

Teams Management

This service includes administration for eligible Microsoft Teams environments, including team and channel management, guest access configuration, meeting policy management, and app permission management. Technicians help ensure Teams remains properly configured for collaboration needs.

Office Applications Management

This service includes support for eligible Microsoft Office applications, including installation support, license activation troubleshooting, feature configuration, and version management. Technicians provide assistance for currently supported versions of Microsoft Office.

Microsoft 365 License Reporting

This service includes reporting on license allocation and usage for eligible Microsoft 365 tenants. Reports are provided through the DivergeIT portal to support cost optimization efforts.

ManageIT PLUS Services

Policy Management

This service includes remote management of existing Microsoft 365 policies for eligible tenants, including security configurations, compliance rules, Data Loss Prevention settings, and Conditional Access policies. Technicians maintain and adjust policies to support ongoing security and compliance requirements.

Microsoft 365 Licensing Cost Notifications

This service includes proactive cost oversight for eligible Microsoft 365 tenants through threshold alerting, license change notifications, and renewal tracking. Technicians help ensure visibility into licensing costs and upcoming changes.

ManageIT PRO Services

Licensing Auto Clean Up Reconciliation

This service includes automated license optimization for eligible Microsoft 365 tenants, including identification of unused licenses, execution of reclamation workflows, and coordination of license true-ups. Technicians help ensure licenses are allocated efficiently.

AugmentIT Optional Services

Intune Device & Application Management

This service includes remote administration for eligible Microsoft Intune environments to secure and manage devices and applications. Technicians maintain existing mobile device management and mobile application management configurations.

Intune Device Enrollment & Inventory Management

his service includes remote support for device enrollment on eligible Intune environments, including management of enrollment restrictions, device categorization, and removal of stale device records. Technicians help ensure device inventory remains accurate and enrollment processes function properly.

Intune Compliance Policy Management

This service includes management of existing compliance policies for eligible Intune environments to ensure devices meet security standards such as encryption status, OS version, and password complexity. Technicians monitor compliance dashboards, provide alerts for non-compliant devices, and perform remote remediation.

Intune Application Management (MAM)

This service includes administration for eligible mobile applications, including deployment of Store apps from Apple App Store and Google Play, assignment of app protection policies, and management of app configuration policies. Technicians help ensure mobile applications are properly deployed and protected.

Intune Configuration Profiles & Security

This service includes maintenance of existing device configuration profiles for eligible Intune environments, including Wi-Fi settings, VPN profiles, and endpoint protection settings such as BitLocker and Defender. Technicians help ensure device configurations remain current and secure.

Intune Remote Device Actions

This service includes execution of remote device actions upon authorized request for eligible devices, including device locking, password resets, and corporate data wipes. Technicians perform actions based on client instructions, including selective corporate wipes for Bring Your Own Device scenarios.

Microsoft Copilot Management

This service includes administration and support for eligible Microsoft Copilot deployments, including license assignment, user enablement, and policy configuration. Technicians assist with Copilot access issues and feature configuration within supported Microsoft 365 applications.

Google Workspace User Support & Management

ManageIT CORE Services

User Management

This service includes remote administration for eligible Google Workspace user accounts, including account creation, license assignment, group management, and role delegation. Technicians handle routine moves, adds, and changes for existing workflows.

Service Health & Incident Management

This service includes monitoring Google Workspace service status for eligible tenants, communicating incidents to stakeholders, coordinating with Google support, and assessing impact. Technicians help ensure visibility into platform health and support response efforts during service disruptions.

Email & Gmail Management

This service includes administration for eligible Gmail environments, including user mailbox management, shared mailbox and group configuration, mail routing rule management, and retention policy configuration. Technicians help ensure email services remain properly configured and operational.

Google Drive Management

This service includes administration for eligible Google Drive environments, including shared drive management, permission configuration, storage quota management, and external sharing configuration. Technicians help ensure cloud storage services are properly maintained.

Google Meet & Chat Management

This service includes administration for eligible Google Meet and Chat environments, including space and group management, guest access configuration, meeting policy management, and app integration management. Technicians help ensure collaboration tools remain properly configured.

Google Workspace Applications Management

This service includes support for eligible Google Workspace applications, including Docs, Sheets, Slides, and Forms. Technicians assist with access issues, feature configuration, and version management.

ManageIT PLUS Services

Policy & Security Management

This service includes remote management of existing Google Workspace policies for eligible tenants, including security configurations, compliance rules, Data Loss Prevention settings, and Context-Aware Access policies. Technicians maintain and adjust policies to support ongoing security and compliance requirements.

ManageIT PRO Services

Google Gemini Management

This service includes administration and support for eligible Google Gemini deployments, including license assignment, user enablement, and policy configuration. Technicians assist with Gemini access issues and feature configuration within supported Google Workspace applications such as Gmail, Docs, Sheets, Slides, and Meet.

Signature Management

ManageIT CORE Services

Support & Troubleshooting

This service includes remote support and troubleshooting for eligible Exclaimer environments. Technicians assist with resolving signature display issues, delivery problems, and platform errors to help ensure signatures function as intended.

User & Group Support

This service includes remote management of signature assignments for eligible Exclaimer environments, including signature policy assignment based on directory attributes, group-based rules, and exception management. Technicians help ensure the correct signatures are applied automatically based on existing workflows.

ManageIT PLUS Services

Annual Policy/Change Management

This service includes Annual signature policy configuration for eligible Exclaimer environments, including modification of existing templates, change approval workflows, and rollout coordination. Technicians help ensure signature policies remain current and properly deployed.

ManageIT PRO Services

As Needed Annual Policy/Change Management

This service includes signature policy configuration for eligible Exclaimer environments, including modification of existing templates, change approval workflows, and rollout coordination. Technicians help ensure signature policies remain current and properly deployed.

Email Disclaimer Management

This service includes technical implementation of legal disclaimers and regulatory compliance footers within eligible Exclaimer signatures, including audit trails and rule verification. Technicians configure compliance elements based on legal text provided by the client.

SecureIT Products

SecureIT CORE Services

Email Security & Hygiene Management

Email Security Management includes configuration and ongoing management of email protection policies (anti-spam, anti-malware, anti-phishing) for Microsoft Defender for Office 365 and Google Workspace, quarantine monitoring and user notification, safe/blocked sender list maintenance, and email authentication protocols (SPF, DKIM, DMARC). Technicians proactively tune policies based on threat intelligence and client communication patterns, conduct annual email security posture reviews, monitor for spoofing and impersonation attempts, and maintain proper authentication to prevent unauthorized use of client domains and improve deliverability.

DNS-Layer Filtering

DivergeIT provides DNS-based security filtering using Todyl to block malicious domains and inappropriate content before connections are established.

DNS-Layer Filtering (SDNS)

DNS-based security filtering management includes DNS query filtering and logging, category-based content blocking, malicious domain blocking, policy customization by user or group, and reporting and analytics. Technicians proactively tune policies based on organizational needs and threat intelligence, review bypass requests and security events, and conduct annual policy effectiveness reviews.

Endpoint Detection & Response (EDR)

Endpoint protection management includes real-time endpoint monitoring and alerting, automated threat detection policy configuration, threat intelligence integration, and investigation tools. Technicians tune detection policies and response automation based on threat landscape changes, coordinate alert triage and remediation actions, and conduct annual endpoint security posture reviews.

Next Generation Antivirus (NGAV)

AI-powered protection beyond traditional signature-based detection includes machine learning-based threat analysis, behavioral monitoring, zero-day threat prevention, fileless malware protection, ransomware prevention, and real-time protection updates. NGAV stops threats that traditional antivirus misses.

Malware Detection & Incident Response

Malware incident management includes detection alerting, remediation coordination, and communication throughout the incident lifecycle. Technicians coordinate containment actions and guide remediation steps to minimize the impact of malware infections.

Behavioral Analysis & Zero-Day Threat Prevention

Advanced threat prevention through behavioral analysis includes user and entity behavior analytics (UEBA), anomaly detection, zero-day exploit prevention, advanced persistent threat detection, and machine learning model updates. Behavioral analysis detects threats based on suspicious patterns rather than known signatures.

SecureIT PLUS Products

Managed Detection & Response

DivergeIT provides 24/7 security operations using Todyl's security platform with expert threat detection and response. Security operations team members monitor client environments and respond to threats around the clock.

Managed Detection and Response (MxDR)

24/7 security operations through Todyl includes continuous security monitoring, expert threat analysis, proactive threat hunting, incident investigation and response, endpoint isolation capabilities, monthly security reports, and security recommendations. Security operations team members provide enterprise-grade security operations and rapid response to detected threats.

Network Security & Access Control (SASE)

Secure Access Service Edge implementation through Todyl includes cloud-based security architecture, Zero Trust Network Access, secure web gateway, cloud access security broker, network traffic analysis, and policy-based access control. SASE provides comprehensive network security for modern distributed workforces.

Microsoft Secure Score Posture Management

Optimization of Microsoft security configuration includes Secure Score monitoring, improvement recommendations, implementation assistance, progress tracking, benchmark comparison, and regular posture reviews. Technicians help strengthen Microsoft 365 security posture through continuous improvement efforts.

Security Breach Incident Response

Response services for confirmed security breaches include incident containment, evidence preservation, root cause analysis, remediation execution, recovery coordination, and post-incident reporting. Security team members provide rapid, expert response to minimize breach impact.

Cloud Security Incident Response

Specialized incident response for cloud environments includes cloud-specific incident handling, multi-cloud investigation capabilities, cloud configuration remediation, identity compromise response, data exposure assessment, and cloud security hardening. Cloud expertise ensures effective response to cloud security events.

SecureIT PRO Products

Zero Trust Segmentation (LZT)

Micro-segmentation implementation for Zero Trust architecture includes network segmentation design, micro-segmentation implementation, policy development, traffic flow analysis, lateral movement prevention, and compliance mapping. Segmentation limits the blast radius of security incidents.

Security Information & Event Management

DivergeIT provides centralized security logging and analytics using Todyl's integrated SIEM capabilities, enabling threat detection and automated response.

Central Logging & Analytics (SIEM 30 Days)

Centralized security event collection with 30-day retention through Todyl SIEM includes log collection from multiple sources, real-time event correlation, security analytics dashboards, custom detection rules, and compliance reporting. Centralized logging enables effective threat detection and investigation.

Security Automation & Response (SOAR)

Automated security orchestration through Todyl includes automated incident response playbooks, security workflow automation, integration with security tools, case management, metrics and reporting, and continuous improvement. Automation accelerates response and ensures consistent handling of security events.

Governance, Risk & Compliance *

DivergeIT provides security governance and compliance management services to help organizations meet regulatory requirements and manage security risk.

Governance, Risk and Compliance Ready *

Foundation for meeting regulatory requirements includes compliance framework mapping, control implementation guidance, gap analysis, remediation planning, audit preparation support, and continuous compliance monitoring. Technicians help navigate complex compliance requirements.

Critical Security Patch Alerts

Proactive notification of critical vulnerabilities includes vulnerability feed monitoring, critical patch identification, impact assessment, prioritized alerting, remediation guidance, and tracking to closure. Rapid awareness of critical vulnerabilities enables timely remediation.

Firewall Rule Reviews & IDS/IPS Monitoring

Security review of firewall configurations using Todyl includes periodic firewall rule review, rule optimization recommendations, IDS/IPS alert monitoring, false positive tuning, threat correlation, and policy documentation. Regular reviews ensure firewall configurations remain effective and secure.

Dark Web Monitoring Notifications

Monitoring for data exposure on the dark web includes credential monitoring, data leak detection, brand mention monitoring, alert notification, risk assessment, and response recommendations. Early detection of exposed credentials enables rapid response.

Dark Web Forced Password Rotation

Automated response to dark web credential exposure includes exposed credential identification, automated password reset triggers, user notification, compliance documentation, trending and analytics, and executive reporting. Automated response reduces the window of opportunity for attackers.

Risk Scoring & Automated Policy Enforcement

Risk-based security posture management includes continuous risk assessment, risk score calculation, automated policy application, exception management, trending analysis, and board-level reporting. Risk scoring helps prioritize security investments.

Anomaly Detection & Threat Intelligence Integration

Advanced analytics with external threat intelligence through Todyl includes behavior-based anomaly detection, threat intelligence feed integration, indicator of compromise matching, proactive threat alerts, investigation support, and intelligence sharing. Threat intelligence enhances detection of emerging threats.

ComplilT Products

*ComplilT CORE Products **

Antivirus & Endpoint Protection Deployed

Documentation of endpoint protection deployment includes verification of antivirus agent presence on all endpoints, policy configuration records aligned with security best practices, automated definition update logs, and continuous threat detection monitoring records. Documentation provides audit evidence that endpoint protection is configured, managed, monitored and effective to meet applicable controls.

Email Filtering (EOP) Configured

Verification of Exchange Online Protection configuration includes spam filter tuning documentation, malware scanning configuration records, quarantine management logs, and policy tuning records. Documentation proves that email filtering is compliant with applicable controls.

Basic Backups Scheduled and Monitored

Ongoing validation of backup operations includes backup job schedule documentation aligned with recovery objectives, daily monitoring logs of backup success and failure, alerting configuration records, and retention policy implementation documentation. Records provide audit evidence of regular, monitored backups for business continuity and recovery.

OS & Application Patching Enabled

Tracking and reporting of systematic patching includes patch policy documentation, automated update scheduling records, compliance monitoring reports identifying unpatched systems, and patch status reporting. Documentation provides audit evidence that patching is occurring in compliance with written patch policy.

Asset Inventory Captured (Devices and Software)

Maintenance of comprehensive IT environment documentation includes hardware inventory reports covering all computers, servers, and network devices, software inventory records, asset documentation with key attributes and ownership, and inventory refresh tracking. Documentation provides audit evidence that asset inventory is maintained and current in compliance with applicable controls.

Standardized Onboarding/Offboarding Checklist

Documentation of consistent user lifecycle management includes onboarding checklists ensuring new users receive appropriate access and equipment, offboarding checklists ensuring timely access revocation and asset recovery, process compliance records, and continuous improvement tracking. Documentation provides audit evidence that user lifecycle management processes are documented and followed in compliance with applicable controls.

SLA Tracking with Performance Reporting

Monitoring and reporting of service level achievement includes SLA metric tracking for response and resolution times, performance dashboard records, trend analysis reports, and monthly performance summaries. Documentation provides audit evidence of accountability and continuous improvement.

Basic Documentation for Systems and Vendors

Maintenance of foundational IT documentation includes system documentation covering configurations and procedures, vendor contact information for escalation and support, network diagrams illustrating infrastructure topology, and runbooks for common procedures. Documentation provides audit evidence that IT systems and vendor relationships are documented in accordance with applicable requirements.

Starter IT Policy Templates

Policy framework documentation includes acceptable use policy defining appropriate technology use, password policy establishing authentication requirements, security policy templates covering key

security controls, and policy customization guidance tailored to compliance framework requirements. Documentation provides audit evidence that policies are established and customized to meet organizational compliance goals and applicable standards.

Cybersecurity Insurance Evaluation

Support documentation for cybersecurity insurance requirements includes completed insurance questionnaires, security control documentation demonstrating security posture, gap identification reports, and remediation guidance. Documentation demonstrates security controls required by insurers for audit and underwriting purposes.

Non-Compliant Device Reporting

Ongoing review and reporting of devices not meeting security standards includes compliance scan results against defined security baselines, non-compliant device reports with specific issues noted, remediation request submissions for identified gaps, and compliance trending reports. Documentation provides audit evidence of visibility and remediation efforts.

*ComplilT PLUS Products **

Backups Tested

Periodic validation and documentation of backups include scheduled recovery test records verifying backup integrity and recoverability, test result reports providing evidence of backup effectiveness, remediation request submissions for identified issues, and RTO/RPO validation documentation. Records provide audit evidence that backups will work when needed most.

Compliance Checklist (CIS/NIST) Completed Annually

Annual compliance assessment and gap analysis includes evaluation results against CIS Controls or NIST Cybersecurity Framework, gap identification reports noting areas not meeting framework requirements, prioritized remediation recommendations with remediation request submissions, and compliance status documentation. Records provide audit evidence of security maturity and framework alignment.

MFA Enforced on Key Systems

Verification and documentation of multi-factor authentication enforcement include MFA configuration records for Microsoft 365 and other key applications, conditional access policy documentation requiring MFA for sensitive access, user enrollment tracking, and exception management records. Documentation provides audit evidence that MFA is enforced in accordance with applicable security requirements.

Monthly Vulnerability Scans

Ongoing vulnerability monitoring and reporting includes external vulnerability scan reports, vulnerability identification documentation, risk-based prioritization records, and remediation tracking with remediation request submissions for critical findings. Documentation provides audit evidence of a proactive vulnerability management program.

Core Policies Deployed (AUP, Access, Incident)

Policy deployment documentation and tracking include Acceptable Use Policy governing technology use, Access Control Policy defining authorization requirements, Incident Response Policy establishing procedures for security events, and policy communication records ensuring staff awareness. Documentation provides audit evidence of governance and compliance requirements.

Annual Advanced Risk Assessment Report

Annual risk assessment documentation and analysis include identified technical threats and vulnerabilities relevant to the organization, risk analysis evaluating likelihood and impact, prioritized

remediation recommendations with remediation request submissions, and executive summary suitable for leadership and board reporting. Documentation provides audit evidence that risk assessments are conducted annually in accordance with applicable frameworks.

Asset Lifecycle Tracking and License Compliance

Ongoing tracking and documentation of asset and license compliance includes device age and warranty tracking records, refresh cycle planning documentation, software license compliance tracking, and procurement recommendation documentation. Records provide audit evidence that asset lifecycle and software licensing are tracked and compliant with applicable requirements.

Periodic Backup Validation and RTO/RPO Documented

Testing and validation records include recovery test documentation using Datto's verification capabilities, RTO and RPO documentation confirming recovery objectives, test result records for compliance purposes, and remediation request submissions for identified issues. Documentation provides audit evidence and demonstrates recovery capabilities.

Infrastructure Monitoring Deployed (CPU, disk, uptime)

Ongoing monitoring and alerting documentation include CPU, memory, and disk utilization monitoring logs, uptime and availability tracking records, threshold-based alerting configuration documentation, and infrastructure health dashboard records. Documentation provides audit evidence that infrastructure monitoring is operational, and reviews are performed to identify areas for improvement.

Basic Change Management Process Implemented

Change management process documentation and tracking includes change request documentation and approval records, scheduled maintenance window documentation, rollback planning records, and change documentation for audit purposes. Documentation provides audit evidence that a change management process is implemented and followed in accordance with applicable requirements.

Compliance Policy Enforcement & Remediation

Ongoing compliance monitoring and enforcement tracking includes automated compliance scan results, policy enforcement logs preventing non-compliant access, remediation workflow documentation with remediation request submissions, and exception tracking for approved deviations.

*ComplIT PRO Products **

Compliance Trend Analysis & Risk Scoring

Ongoing compliance analysis and risk scoring includes historical compliance trending reports showing improvement over time, risk score calculation records, improvement recommendations with remediation request submissions based on trends, and executive reporting suitable for leadership. Documentation provides audit evidence helping focus security investments based on trend analysis.

Mapped to Policy & Evidence for HIPAA, CMMC, or ISO

Framework-specific control mapping and evidence packages include control mapping documentation to HIPAA, CMMC, ISO 27001, or other applicable frameworks, evidence documenting control implementation, gap analysis reports identifying areas requiring improvement with remediation request submissions, and remediation planning documentation. Framework-specific mapping provides auditors and regulators with required compliance evidence.

DR Tests and Backup Validation

Comprehensive disaster recovery testing and documentation includes quarterly disaster recovery exercises, Datto backup validation documentation, recovery time testing results against RTO

objectives, and documented evidence for compliance purposes. Documentation provides auditors with evidence of disaster recovery capabilities.

Security Training Tracked for All Users

Security awareness training tracking and reporting includes training assignments and completion records for all users, completion monitoring and follow-up documentation, training records maintained for compliance evidence, and periodic refresher training records. Documentation provides audit evidence that security awareness training is assigned, tracked, and completed in accordance with applicable requirements.

Vendor Risk Assessments Documented

Third-party risk management documentation and tracking include completed vendor security questionnaires for critical vendors, risk assessment documentation evaluating vendor security, periodic reassessment records, and remediation tracking with remediation request submissions for identified concerns. Documentation provides audit evidence that vendor risk assessments are conducted and documented in accordance with applicable frameworks.

Annual Compliance Audit Support

Audit preparation coordination and evidence packaging includes evidence gathering and organization, auditor liaison and response documentation, gap remediation support with remediation request submissions, and audit preparation materials. Support streamlines the audit process and improves audit outcomes through comprehensive evidence packages.

Custom Policy Set Enforced

Comprehensive policy framework support includes custom policy development tailored to organizational and regulatory requirements, policy deployment and communication documentation, compliance monitoring and enforcement records, and periodic policy review and updates. Engineers assist with maintaining and updating policies to accurately reflect organizational practices and evolving compliance requirements.

Full ITAM System with Procurement-to-Retire Workflow

Comprehensive IT Asset Management tracking and documentation includes centralized asset repository records tracking all hardware and software, procurement workflow documentation from requests through acquisition, deployment tracking and configuration management records, and retirement workflow documentation ensuring secure disposal and license recovery. Evidence provides auditors with complete asset lifecycle visibility and control documentation.

Backup Verification and Documented Restore Logs

Rigorous backup verification and restore logging includes regular restore testing records, verification logs maintained for compliance evidence, issue tracking with remediation request submissions, and executive reporting on backup program health. Documentation provides auditors with confidence in recovery capabilities.

Change Reviews and Rollback Planning

Change management maturity reviews and documentation includes periodic review records of changes and their outcomes, rollback planning and testing documentation for critical changes, change success metrics and trending reports, and continuous improvement documentation. Evidence demonstrates processes minimizing risk from changes.

Architecture Diagrams and Vendor Documentation

Comprehensive technical documentation maintenance and updates include current architecture diagrams showing system relationships, vendor documentation covering contracts, contacts, and SLAs, integration documentation for connected systems, and regular update records ensuring

documentation remains current. Documentation provides auditors with complete technical environment understanding supporting audit requirements.

IT Performance and Capacity Planning Reviews

Strategic IT planning reviews and reporting include quarterly performance review records assessing system health, capacity planning documentation ensuring adequate resources for growth, budget planning for infrastructure investments, and executive reporting on IT performance and plans.

Custom SIEM & IR Playbooks in Place

Advanced security operations documentation and validation include custom SIEM rule documentation tailored to the environment, incident response playbooks for common scenarios, documented escalation procedures, and regular playbook review and update records. Evidence packages demonstrate detection and response capabilities tailored to specific risks for audit purposes

LeadIT Products

LeadIT Manager

Leads Technical Business Reviews

Scheduled tactical reviews are conducted to analyze ticket trends, service performance metrics, and near-term hardware and software requirements. Reviews provide actionable insights to address recurring issues, identify service improvement opportunities, and plan for upcoming technology needs.

Coordinates & Collaborates with all IT Vendors

Acts as the primary technical liaison for third-party internet, phone, and software vendors. This includes coordinating troubleshooting efforts, escalating issues on behalf of the client, and ensuring vendor accountability for service delivery and resolution timelines.

Document User Onboarding and Offboarding Processes

Standardized technical checklists are maintained for provisioning new employees and de-provisioning departing staff. Documentation ensures consistent access setup, security compliance, and efficient transitions while reducing the risk of orphaned accounts or unauthorized access.

Maintains IT Asset Inventory and Lifecycle Plans

Hardware and software asset age, warranty status, and location are tracked for eligible devices to identify assets approaching end-of-life. Lifecycle planning supports proactive refresh recommendations, warranty claim coordination, and budget forecasting for hardware replacements.

LeadIT Director

IT Budget Tracking & Quarterly Variance Reporting

Actual IT expenditures are tracked against the established budget and variances are reported on a quarterly basis. Reporting identifies cost overruns, underspend opportunities, and trends to support informed financial decision-making and budget adjustments.

Coordinates with all IT Vendors & Licensing

Vendor relationships are managed with a focus on license compliance, contract renewal dates, and consolidation opportunities. Proactive license management helps avoid compliance penalties, eliminates redundant subscriptions, and identifies cost-saving opportunities across vendors.

Creates IT Health Summary Report

A comprehensive scorecard is delivered summarizing infrastructure health, security posture, support performance, and asset currency. Reports provide visibility into the overall state of the IT environment, highlight areas requiring attention or investment, and include recommendations for improvement.

Manages Annual IT Spend Forecast & Cross-Vendor Budget

A comprehensive annual IT budget forecast is developed consolidating MSP fees, hardware refreshes, and third-party software subscriptions. Forecasting enables accurate financial planning, supports capital expenditure requests, and aligns IT spending with organizational priorities.

Reviews IT Project ROI and Business Case Alignment

Proposed IT projects are evaluated to ensure they deliver measurable operational value and align with budget priorities before approval. Reviews include cost-benefit analysis, risk assessment, alignment with strategic objectives, and post-implementation benefit tracking to support sound investment decisions.

LeadIT Executive

Aligns Technology Roadmap with Business Objectives

Organizational goals such as geographic expansion, mergers and acquisitions, and remote workforce shifts are translated into a multi-year technology execution plan. Roadmaps align IT investments with business priorities and ensure technology enables rather than constrains growth.

Owns Multi-Year IT Strategy and Stakeholder Alignment

A 3-5 year strategic IT vision is developed with buy-in from key internal stakeholders and department heads. Strategic planning ensures cross-functional alignment, prioritizes initiatives based on business impact, and establishes clear technology direction for the organization.

Represents IT at Executive/Board Meetings

Technology advisory services are provided during board or executive sessions including preparation of board-level presentations and materials, presentation of strategy, risk assessments, and investment requirements, and response to executive inquiries on technology matters. Representation ensures leadership has the information needed to make informed decisions about technology investments and risk tolerance.

Develops Business Continuity/Disaster Recovery Plans

Comprehensive BC/DR frameworks and recovery strategies are designed to ensure organizational resilience during major disruptions. Planning includes risk analysis, recovery time objectives, failover procedures, regular plan reviews, and coordination of plan testing and exercises to maintain readiness.

Advises on Regulatory Frameworks *

Strategic guidance is provided on aligning IT controls with relevant industry regulations such as HIPAA, CMMC, and ISO. Advisory services help identify compliance gaps, prioritize remediation efforts, and ensure technology practices support audit readiness and regulatory obligations.

<u>* Ultimate Responsibility for Compliance</u>

Client acknowledges and agrees that, while Provider will use its best efforts to assist Client in complying with the technical requirements of applicable regulatory rules, Client remains ultimately responsible for its own compliance with all applicable laws, regulations, and industry standards.