GET STARTED WITH STORM REPLY, YOUR NEXT-GEN MANAGED SERVICE PROVIDER

A next-gen AWS MSP is committed to three key tenets: educate customers on a proactive, ongoing basis, offering consultative and advisory services, lead with AWS Professional Services, just like a systems integrator (SI) would, and advocate to customers the use of and evolution of AWS services.

STORM REPLY is specialized in the design and implementation of innovative Cloud-based solutions and services. Through consolidated expertise in the creation and management of Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) Cloud solutions, Storm Reply supports important companies in Europe and all over the world in the implementation of Cloud-based systems and applications. Storm Reply is AWS Premier Consulting Partner.

www.reply.com

MANAGED SERVICE PROVIDER

Typically, a managed service provider (MSP) is a type of IT service company that provides server, network, and specialized applications to end users and organizations. Normally these applications are hosted and managed by the service provider.

Managed service providers tend to be Web hosting or application service providers that allow customers of different sizes to outsource their network and application resource procedures under a delivery agreement. In most cases, MSPs own the entire physical back-end infrastructure and provide resources to end users remotely over the Internet on a self-service, on-demand basis.

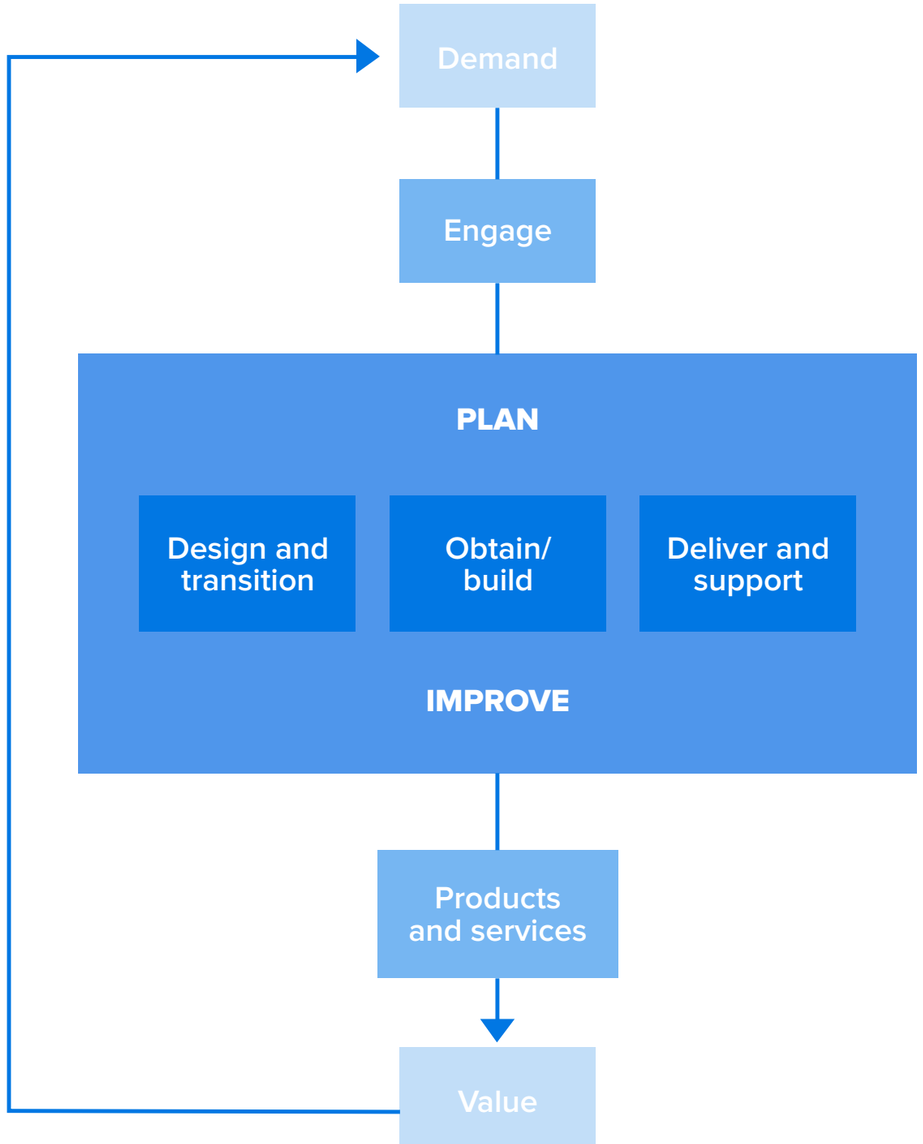
Managed service providers monitor, supervise and secure outsourced network or application procedures on behalf of the organizations that are using those services. MSPs have specialized infrastructure, human resources and industry certifications, and they provide 24/7 monitoring and provisioning of additional services for their customers.

STANDARD MSP SERVICES

IT asset management	To plan and manage the full lifecycle of all IT assets, to help the organization maximize value; control costs; manage risks; support decision-making about purchase; re-use, and retirement of assets; and meet regulatory and contractual requirements.
Monitoring and event management	To systematically observe services and service components, and record and report selected changes of state identified as events, through identifying and prioritizing infrastructure, services, business processes, and information security events, and establishing the appropriate response to those events, including responding to conditions that could lead to potential faults or incidents.
Service level management	To set clear business-based targets for service performance, so that the delivery of a service can be properly assessed, monitored, and managed against these targets.
Change control	To maximize the number of successful IT changes by ensuring that risks have been properly assessed, authorizing changes to proceed, and managing the change schedule.
Problem management	To reduce the likelihood and impact of incidents by identifying actual and potential causes of incidents, and managing workarounds and known errors.
Service Desk Management -SPOC	To capture demand for incident resolution and service requests. It should also be the entry point and single point of contact for the service provider with all of its users.
Service request management - HD1	To support the agreed quality of a service by handling all pre-defined, us-er-initiated service requests in an effective and user-friendly manner.
Availability Management	To ensure that services deliver agreed levels of availability to meet the needs of customers and users.
Incident management	To minimize the negative impact of incidents by restoring normal service operation as quickly as possible.
Release management	To make new and changed services and features available for use.
Service validation and testing	To ensure that new or changed products and services meet defined requirements. The definition of service value is based on input from customers, regulatory requirements, and is documented as part of the value chain activity of design and transition. These inputs are used to establish measurable quality indicators that support the definition of assurance criteria and testing requirements.

Continual improvement	To align the organization's practices and services with changing business needs through the ongoing identification and improvement of services, service components, practices, or any element involved in the efficient and effective management of products and services.
Information security management	To protect the information needed by the organization to conduct its business. This includes understanding and managing risks to the confidentiali-ty, integrity, and availability of information, as well as other aspects of in-formation security such as authentication and non-repudiation.
Measurement and reporting	To support good decision-making and continual improvement by decreasing the levels of uncertainty. This is achieved through the collection of relevant data on various managed objects and the valid assessment of this data in an appropriate context.
Relationship management	To establish and nurture the links between the organization and its stakeholders at strategic and tactical levels. It includes the identification, analysis, monitoring, and continual improvement of relationships with and between stakeholders.
Deployment management	To move new or changed hardware, software, documentation, processes, or any other component to live environments. It may also be involved in deploying components to other environments for testing or staging.
Infrastructure and platform management	To oversee the infrastructure and platforms used by an organization. When carried out properly, this practice enables the monitoring of technology solutions available to the organization, including the technology of external service providers.
Service configuration management	To ensure that accurate and reliable information about the configuration of services, and the configuration items (CIs) that support them, is available when and where it is needed. This includes information on how CIs are configured and the relationships between them.

Through these practices, MSP providers are able to tap into the Service Value Chain and boost the added value at the end of each step, in order to promote the customer business.



NEXT GENERATION SERVICE PROVIDER

Next-Gen MSP is a Managed Service Provider which takes the practices described above and brings them to the next level by focusing on the added value of Cloud-based services.

Key concepts:

Hardware to Software: By migrating away from on-premises hardware to cloud-based solutions, next-gen MSPs and their clients no longer have to worry about fixing a server that's gone down or refreshing their technology at regular intervals. Instead, they can focus on the software and cloud services that best help them achieve their business needs.

Centralized to Distributed: Traditional MSPs often use a "fishbowl" network operations center, in which a team provides services from a centralized location. Next-gen MSPs are moving away from this model in favor of a decentralized, automated setup. Intelligent, self-healing, cloud-native solutions can remove a great deal of the manual work that the fishbowl model requires.

Disorder to DevOps: Change management for traditional MSPs can be a highly complex operation due to the great deal of manual work that it requires. A growing number of next-gen MSPs are using DevOps to implement and track changes more efficiently. By pushing new code into production more quickly, next-gen MSPs can make your business more agile and improve ROI.

Vendor to Advisor: Perhaps most importantly, MSPs are becoming less about tech support and more about long-term strategic consulting to help you reach your potential as a business. Next-gen MSPs take full ownership of and responsibility for your destiny as a company. They understand that it's not about the technology itself, but how you use it to get where you want to be.

Next-Gen MSP develop and provide to their customer a Cloud Center of Excellence, made up by as follow.

CCOE Team	Roles and Responsibility
Alliance Team	Owns the AWS relationship; conducts opportunity mapping.
Support/Operation Team	Provides Tier 1-3 support, and acts as the primary technical contact for customers.
Sales Team	Engages with customers on initial and ongoing cloud opportunities.
Marketing Team	Develops and delivers messaging focused on differentiations and areas of expertise.
Professional Services and Delivery Team	Provides strategic engagement and consultation services.
Solution Architecture Team	Designs solutions for customers.

Next-Gen MSP operates dev first, by default, by design. Automation on all level is key to the added value of the MSP provider. These two goals are achieved with the full adoption of:

Dev(Sec)Ops framework to enable customers to solve their business problems;

Infrastructure As Code to ensure repeatable, testable, auditable, consistent infrastructure deployments;

Testing and auditing of produced artifacts;

Tooling to ensure customer doesn't need to maintain their own tool: CICD, Backup/Restore, Data Migration, Workflow automation Cost-saving through instance scheduling;

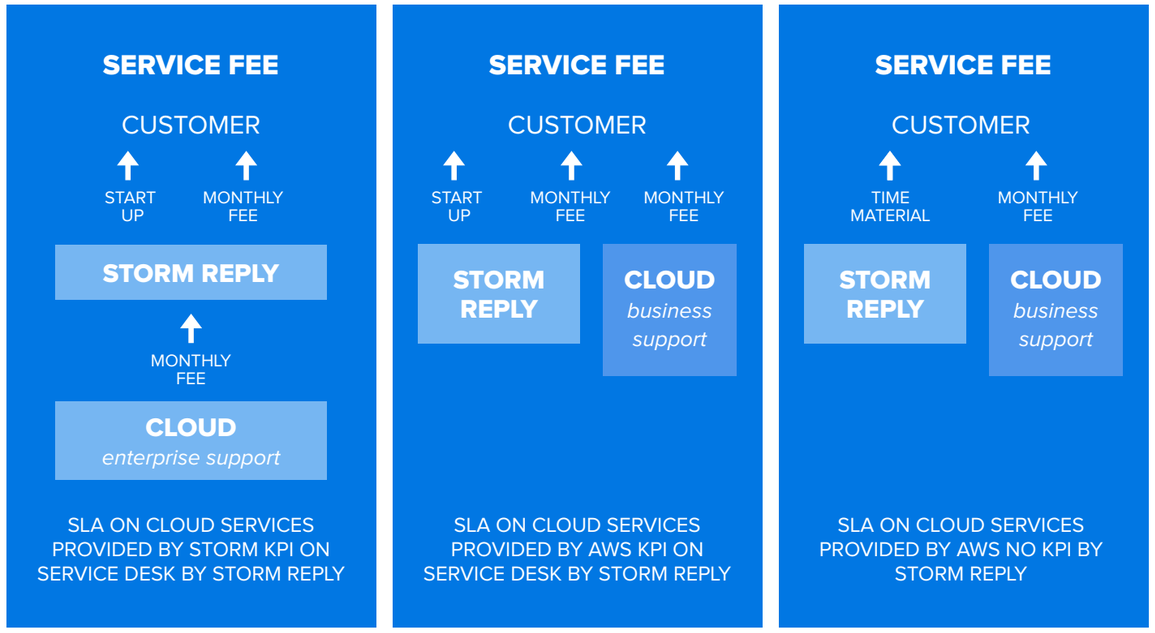
Training and Continuous Improvement to ensure customer integration with MSP tools.

THE ADDED VALUE OF STORM REPLY

Storm Reply is an AWS Premier Consulting Partner since 2014, ranked in the top 10 globally, and one of the few companies to have so many different competencies attested by AWS: Security, Financial Services, SaaS, Data & Analytics, DevOps, Machine Learning, Industrial Software, IoT, Migration, Oracle.

Storm Reply is also partner for AWS Managed Service Provider program since 2013 and AWS Well-Architected program since 2018. These credentials provide us with an experienced background of design, development, deployment and operations of cloud-based solutions for many customers in different industries.

Our in-house service team is composed by multiple more than 30 certified units such Cloud Operations, Incident Response Team, Cloud Architects, Dev/SysOps engineers. This structure allows us to be agile and flexible in supporting the business needs of our clients. Our standard offering is usual articulated into three main possibilities.



THE ONBOARDING PROCESS

The on-boarding process is the standard workflow framework developed, consolidated and adopted by Storm Reply with the goal of taking in charge a customer workload on AWS.

The output of this framework is to make an inventory of the assets, define processes and procedures, review the documentation, assess the security posture of the system, check the monitoring system, integrate alerting with 24/7 operations and take in charge the responsibility to operate a customer workload.

The scope is to define the perimeter of the systems in charge, identify possible service gaps (GAP analysis) and put in place a strategy plan to close them.

The process is structured as follow.

LITE ASSESSMENT

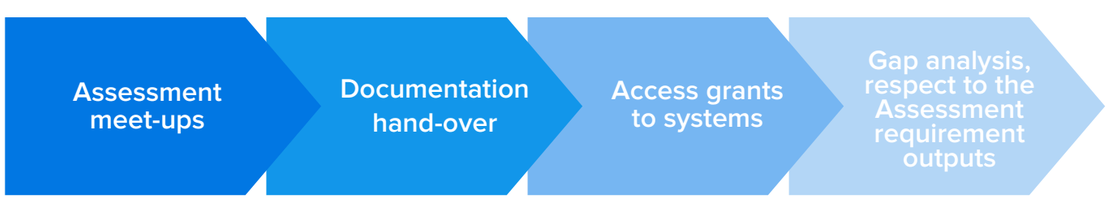
The Lite assessment activity aims to quickly gather basic information on a system and provide a rough estimation of the service. We provide a form with standard questions to be filled in by the customer in and based on that information and some assumption on the solution we provide a rough estimation.

This can be used as starting point to plan the full assessment and tailor the management offer accordingly. The Lite assessment activity typically takes one business day.

FULL ASSESSMENT

The full assessment activity aims to define the as-is baseline of the current deployed infrastructure and produce a GAP analysis. The collected information helps define and tune a service management proposal for the customer specific perimeter.

Information can be collected through interviews, workshops, remote meeting, depending on the scope of the service. The full assessment activity typically takes five business days.



The minimum information needed is:

Asset inventory

- Number of AWS accounts
- Number of EC2 instances
- Number of RDS databases
- Number of ECS clusters
- Number of EMR clusters
- Number of EKS clusters
- Number of Serverless Apps
- Number of Redshift clusters
- Number of CICD pipelines

Document inventory

- Architecture documents
- Architecture diagram
- Architecture layers description of the technology stack
- Networking documents
- Communication flow documents
- RACI Matrix
- Playbook and operations documents
- Application deployment documents
- Change management documents
- Incident management documents
- Service Request management documents

Governance requirements

- RPO and RTO
- Backup retention policy
- Availability
- Disaster Recovery

Monitoring requirements

- Infrastructure
- Application
- Performance

Security requirements

- User access levels
- Antimalware
- WAF
- PKI
- Encryption
- User authorization and authentication
- Firewal

Once the above information is gathered, the following steps are:

1. Perform the full assessment in the agreed form (workshops, interviews, remote meetings, etc.)
2. Handover of the documentation discovered in the assessment phase
3. Gather access to the systems in scope to deliver the service:
   - Infrastructure
   - Ticket Trouble System
   - Monitoring
   - CICD
   - Third-Party tools
4. GAP analysis on the collected information. The output is a list of action items to be addressed before the service can start.

ONBOARDING AND SERVICE SETUP

The onboarding activity goal is to close the highlighted gaps for the service takeover and define together with the client the management procedures that will dictate the running phase. The time to complete this phase heavily depends on the outcome of the GAP analysis, but usually the activity can be completed within one month.

The steps for setup are:

1. Onboarding workshop with the client to present assessment and GAP analysis results. In this meeting the service model, engagement paths, service levels agreements and an onboarding timeline by component (milestones) will be presented
2. The GAP Recovery plan is then executed
3. After successful implementation of the remediations identified, the managed service can start.

SERVICE RUNNING (BUSINESS AS USUAL)

When previous phase is completed a cut-over deadline is defined together with the client. Starting from this deadline Storm Reply gets ownership and responsibility for the service.

Before this deadline, the service documents and processes are finalized and approved by the client:

- Contact points and escalation matrix
- Ticket Trouble Systems issue type and workflows
- Operational manual for monitoring alarms
- Playbooks and common service requests perimeter
- Incidents report template
- Service review meeting template

A regular service review meeting is then scheduled in order to track service status and discuss improvements to service quality.

After the cutover date, Storm monitors the provided services, checks service levels, produces regular reports on the service quality, promotes service improvements and evolutions, in order to guarantee always the best added value for the client.

LEVERAGE THE TECHNOLOGICAL COMPETITIVE ADVANTAGES OF THE PROVIDER AND TURN IT INTO ADDED VALUE FOR THE END CUSTOMER