1. **Cloud Infrastructure**

To maintain the integrity of cloud infrastructure, all machines and accounts must be password protected, alongside the implementation of 2-Factor Authentication. Not only does this apply a second layer of security to the cloud infrastructure, but log-in attempts can be monitored and logged through the 2FA implementation, ensuring that the company can be made aware in the event of an infrastructural breach in the cloud department. This allows for quick responsiveness in the event of an emergency, thus working to protect sensitive information and network storage.

1. **Application Performance**

A major way to monitor application performance is through user feedback and reviews. Only a user can provide a gauge as to whether the performance needs to be worked on and improved, and what specifically needs to be improved on. An active strive for positive user reviews can help aid this, by swiftly responding to negative and constructive user reviews to provide an adequate experience.

Aside from reviews, load testing can be done on the applications to test for internal performance limitations and scalability issues where server-side upgrades may need to take place if necessary.

Though ultimately, application performance can be monitored through the implementation of technical monitoring metrics, such as response time, error rates and total-resource usage. Application Performance Measurement (APM) solutions much be explored for an in-depth analysis of application performance.

1. **Resource Usage and Cost**

To monitor resource usage, tools such as Datadog or Grafana can be utilized to monitor CPU usage, memory usage, disk activity and network traffic. This information can be used to dictate whether certain areas of operation are under heavy load, and appropriate measures can be taken to come to a solution.

Moreover, to monitor resource costs, budgeting practices must take place to ensure that our resources expenses are managed effectively. To do this, a cost-usage matrix should be created to assess whether it is worthwhile spending a certain amount of money on a resource that we may barely use. By doing so, we can cut out unnecessary resource costs, therefore optimizing our budget allocation.

1. **Security and Compliance**

Not only do we need to adhere to industry standards, but regular checks on full compliance policies need to take place to ensure that these standards are adhered to. This can be monitored through regular risk assessments based on an already defined risk matrix, documenting and reporting any changes and how they were assessed/put in place. All relevant employees must be briefed and trained so they are aware of all security and compliance measures, so they are not compromised at any time. Though these compliance policies and contingency plans must be easily accessible for all staff members in the event of a compliance breach.

1. **Network Performance**

To monitor network performance, real-time bandwidth measurements should regularly be taken to identify if the network is under high load. Applications like Wireshark can then be utilized to investigate network traffic and its impact on performance. This allows the networking team to analyze network traffic in real-time, identifying which connections require additional bandwidth.

Additionally, automated alerts can be set up to send a message to our networking team when there are networking issues, allowing them to identify where the network is underperforming and how to adjust accordingly.

1. **Backup and Disaster Recovery.**

Backup and Disaster recovery can be implemented and monitored through the administration of an automated storage backup program – such as “Microsoft Azure Backup” (though we may need to switch from GCP first), or Veritas NetBackup, which offers automated storage backups for both, on-site and off-site storage.  
  
These storage logs should be regularly reviewed to ensure that all required information is stored safely, and incident response plans should be put in place in the event of the need for Disaster Recovery.

1. **User Activity and Usage**

To monitor user activity and usage, logging mechanisms should be implemented to verify and record user authentication events. These logs will include information such as login attempts (both successful and unsuccessful). This allows the team to determine when an individual is connected to the network, therefore monitoring their usage.

To better monitor activity and usage, Redback Operations can investigate implementing SIEMs to better record activity on devices, servers, applications, and security measures (such as firewalls) in the form of logs.

Moreover, regular audits can take place, reviewing the usage of users (recorded by the logging systems previously explained). This can be used to identify how users navigate the system, what they access and what they have access to, allowing for appropriate changes to be made if required.

1. **System Updates and Patches**

To monitor system updates and patches, patch management software, such as “Windows Server Update Services” or “System Center Configuration Manager” can be utilized to automatically patch and update the Redback Operations servers and systems to actively patch any bugs or exploits. In tandem with this, automatic updates will be provided when a new patch or update is available.

Additionally, the implementation of tools such as “Nessus” or “OpenVAS” can be used to regularly scan for vulnerabilities in the system and server. These scans can then be logged and reported and accurately responded to via a previously explained patch management software.

Finally, we can establish a monitoring/reporting system to track the deployment of patches, allowing us to maintain compliance with security protocols and actively respond to any issues that may arise in the patch deployment phase.