This is a chargeable service

BYTES

Ensuring Compliance and Security

Cloud Configuration Review

At **Bytes**, we provide meticulous Cloud Configuration Review Services for cloud environments including Azure, Microsoft 365, Amazon Web Services (AWS) or Google, tailored to guarantee compliance and bolster security measures. Our assessments align your configurations with industry benchmarks for a secure and compliant cloud environment.

Why Configuration Review Matters:

Evaluating configurations against industry benchmarks such as CIS Benchmark (Level 1 or Level 2) is crucial for ensuring compliance and fortifying security. Our expert assessments ensure your cloud environments adhere to these standards, minimising vulnerabilities and ensuring robust security.

Is Configuration Review Right for You?

Consider a configuration review if maintaining compliance, fortifying security measures, or ensuring adherence to industry standards is vital for your cloud environment.

Secure your cloud environment and ensure compliance with Bytes Cloud Configuration Review Services.

Why Choose Our Cloud Configuration Review Services?

- ✓ **Compliance Assurance:** Ensure adherence to industry benchmarks, meeting regulatory standards and avoiding penalties.
- ✓ **Enhanced Security Measures:** Implement recommended changes to fortify configurations against potential vulnerabilities.
- ✓ **Risk Mitigation:** Proactively address configuration weaknesses to minimize security risks.
- ✓ **Protect Critical Assets:** Safeguard sensitive data and critical assets within your cloud environments.
- ✓ **Continual Compliance:** Maintain ongoing compliance through periodic assessments and updates.

What's Included?

Microsoft

Our Cloud Configuration Review involve essential stages:

Evaluation Against Industry Benchmarks: Thorough assessment of configurations against CIS Benchmark (Level 1 or Level 2) standards.

Analysis of Configurations: Detailed examination of your cloud settings to identify vulnerabilities.

Identification of Compliance Gaps: Pinpoint deviations from industry benchmarks, highlighting potential security risks.

Comprehensive Reporting: Detailed reports outlining assessment findings, compliance gaps, and actionable recommendations for security enhancement.